



승인번호
제 127013호

2019년 12월



2019

국내 정보보호산업 실태조사

Survey for Information Security Industry in Korea : Year 2019



과학기술정보통신부
Ministry of Science and ICT

KISIA 한국정보보호산업협회
Korea Information Security Industry Association



2019 국내 정보보호산업 실태조사

이용자를 위하여

1. 통계표 및 도표내의 숫자는 반올림되었으므로 세부항목의 합이 전체 합계와 일치하지 않을 수 있음
2. 통계표 및 도표에 사용된 기호의 뜻은 다음과 같음
- : 해당숫자 없음 E : 추정치
3. 매출액, 수출액, 인력 등의 통계치는 사후총화를 통해 모수를 추정한 결과값임
4. 복수응답은 한 개 이상을 응답한 결과치를 집계(비가중)한 결과임
5. 본 보고서의 내용을 인용할 때에는 반드시 과학기술정보통신부, 한국정보보호 산업협회(KISIA)의 자료임을 밝혀야 함
6. '19년도 국내 정보보호산업 실태조사는 중분류 기준으로 작성되었음
7. 정보보안 시스템 개발 및 공급 부문의 기타 제품 분류는 삭제되었음

1 연구 과제

2019 국내 정보보호산업 실태조사

2 연구의 목적

본 연구는 2019년 정보보호산업의 시장 조사를 기초로 국내 정보보호산업의 시장규모를 파악하고 향후 전망을 예측하는 것을 주된 목적으로 하며, 나아가 정보보호산업을 육성할 수 있는 정책적 방향을 제시하고자 한다.

3 연구의 내용 및 범위

본 연구는 국내 정보·물리보안산업 관련 기업을 대상으로 일반적 특성, 매출 현황, 수출 현황, 인력 및 고용 현황, 기술개발 현황 및 정부지원요구사항 등을 주요 내용으로 하였으며, 아울러 국내 정보보호산업을 육성할 수 있는 정책방향을 제시하였다.

4 주요 연구결과

○ 정보보호산업 기업현황

국내 소재 정보보호 기업은 정보보안 473개, 물리보안 621개로 총 1,094개로 조사되었다.

[표] 국내 정보보호산업 기업 현황

(단위 : 개)

년도	정보보안	물리보안	합계
2019	473	621	1,094
2018	464	549	1,013
2017	332	565	897
2016	311	553	864

○ 정보보호산업 매출 및 전망

2019년 전체 정보보호산업 매출액은 총 10,557,237백만원으로 2018년 대비 4.3% 증가한 것으로 조사되었다. 정보보안 매출액은 2018년 3,082,926백만원에서 2019년 3,277,687백만원으로 6.3% 증가하였으며, 물리보안 매출액은 2018년 7,034,918백만원에서 2019년 7,279,550백만원으로 3.5% 증가하였다.

[표] 정보보호산업 매출 현황

구분	정보보안			물리보안			합계		
	2017년	2018년	2019년(E)	2017년	2018년	2019년(E)	2017년	2018년	2019년(E)
매출액 (백만원)	2,744,940	3,082,926	3,277,687	6,840,822	7,034,918	7,279,550	9,585,762	10,117,844	10,557,237
성장률 (%)	12.3		6.3	2.8		3.5	5.6		4.3

○ 정보보호산업 수출 및 수출전망

정보보호산업 수출액은 2018년 1,556,132백만원에서 2019년에는 5.8% 증가한 1,646,313백만원이 될 것으로 예상된다. 정보보안 수출액은 2018년 82,363백만원에서 2019년 108,528백만원으로 31.8% 증가하였으며, 물리보안 수출액은 2018년 1,473,769백만원에서 2019년 1,537,785백만원으로 4.3% 증가하였다.

[표] 정보보호산업 수출 현황

구분	정보보안			물리보안			합계		
	2017년	2018년	2019년(E)	2017년	2018년	2019년(E)	2017년	2018년	2019년(E)
수출액 (백만원)	94,398	82,363	108,528	1,475,755	1,473,769	1,537,785	1,570,153	1,556,132	1,646,313
성장률(%)	-12.7		31.8	-0.1		4.3	-0.9		5.8

○ 정보보호산업 인력 및 채용 현황

정보보호산업 인력 수는 총 46,275명(2018년 12월 기준)으로, 이 중 정보보안 인력은 28.9%인 13,378명, 물리보안 인력은 71.1%인 32,897명인 것으로 조사되었다.

[표] 정보보호산업 인력 현황

구분	정보보안	물리보안	합계					총합계(명)
			4년 미만	4년 이상 7년 미만	7년 이상 11년 미만	11년 이상 15년 미만	15년 이상	
인원수(명)	13,378	32,897	13,748	12,334	10,438	6,268	3,487	46,275
비중(%)	28.9	71.1	29.7	26.7	22.6	13.5	7.5	100.0

2019년 정보보호 기업의 신규 채용자는 4,658명이며, 2020년은 4,121명 수준으로 예상된다.

[표] 정보보호산업 채용 현황 및 계획

구분	2019년			2020년 예상		
	정보보안	물리보안	합계	정보보안	물리보안	합계
인원수(명)	1,806	2,852	4,658	1,334	2,787	4,121
비중(%)	38.8	61.2	100.0	32.4	67.6	100.0

○ 정보보호산업 기술개발 현황

정보보호 기업들의 지식재산권 보유 현황을 살펴보면 현재 보유중인 지식재산권이 총 7,093건, 현재 출원 중인 지식재산권이 770건인 것으로 조사되었다.

[표] 지식재산권 보유 현황

(단위 : 건)

구분	현재보유	현재 출원 중
정보보안	2,120	426
물리보안	4,973	344
합계	7,093	770

○ 정보보호산업 정부지원 요구사항

정보보호 시장 활성화를 위한 정부의 정책에 대해서는 ‘자금 지원 및 세제혜택’, ‘공공 부문의 시장수요 창출’, ‘기술개발 지원’, ‘전문인력 양성’ 등의 요구가 높은 것으로 조사되었다.

[표] 정보보호 시장 확대를 위한 정부 지원 필요 사항(복수응답)

(단위 : %)

구 분	정보보안	물리보안
전문인력 양성	18.9	7.1
기술개발 지원	34.1	28.0
기술이전의 활성화	6.8	6.2
법/제도 제 개정	6.5	11.8
공공부문의 시장수요 창출	10.8	9.5
소비촉진/투자활성화	4.3	6.6
자금지원 및 세제혜택	15.8	27.5
해외지원 사업 확대	2.2	2.4
기타	0.6	0.9
합계	100.0	100.0

○ 정책적 시사점

정보보호산업에서 비즈니스 활동을 하는 참여기업 수가 2018년도 1013개에서 2019년도에는 1,094개로 8.0% 증가한 것으로 나타났다. 특히, 물리보안 기업은 549개에서 621개로 증가하였는데, 이는 물리보안분야에서 비즈니스 기회가 많아지고 있기 때문에 기업들의 참여가 높아지고 있다는 것을 의미하고, 그 규모도 커지고 있다는 것으로 해석할 수 있다. 정보보호 기업체 수의 증가는 정보보호시장이 꾸준히 성장하고 있다는 것을 의미한다.

정보보호산업의 성장률은 2017년에는 6.0%, 2018년에는 5.6%에서 2019년에는 4.3% 성장하는 등 매년 성장세가 꾸준히 지속되고 있는 것으로 나타났다. 2018년도에는 정보보호시장 규모는 10조원을 돌파한 것으로 추정되고, 정보보안시장 규모도 3조원 돌파, 물리보안시장 규모도 7조원을 돌파한 것으로 추정된다. 다만, 정보보호시장규모 성장률의 증가폭은 다소 완화되어 향후에도 성장폭은 점점 낮아질 것으로 보인다.

2019년도 정보보안 분야의 성장은 정보보안시스템 개발 및 공급시장이 7.01%, 정보보안 관련 서비스 시장은 6.32% 증가한 것으로 나타나 전체 규모에서는 정보보안시스템 개발 및 공급시장이 훨씬 크고, 최근 성장추세 또한 정보보안시스템 개발 및 공급시장이 주도하고 있는 것으로 나타났다. 향후에도 ISMS 의무화 대상자 확대 등에 따라 보안교육 및 훈련 서비스, 공인/사설 인증서, 보안관제 서비스 시장은 지속적으로 성장할 것으로

예상된다.

정보보호산업의 수출은 2017년의 경우 2016년 대비 12.7% 감소하였고, 2018년에는 전년 대비 0.9% 감소, 2019년에는 전년 대비 5.8% 증가한 것으로 나타났다. 최근 이러한 증가 추세에도 불구하고 수출액은 2015년 1,623,673백만원 수준을 회복하는 정도에 그친 것으로 나타나 지속적인 수출 경쟁력 확보가 필요하다고 판단된다.

정보보호 기업에 종사하는 인력은 2018년 44,029명에서 2019년 46,275명으로 전년 대비 5.1% 증가한 것으로 나타났다. 특히 정보보안 기업에 종사하는 인력이 10.9% 증가한 것에 비해, 물리보안 기업에 종사하는 인력은 2.9% 증가한 것에 그친 것으로 나타나, 정보보안 기업은 시장규모에 비해 상대적으로 더 많은 일자리 증가에 기여하고 있는 것으로 추정된다.

5 기대효과

본 연구를 통해 얻을 수 있는 기대효과는 다음과 같다. 첫째, 정보보호산업에 대한 산업 특성, 매출, 수출, 인력 현황, 시장동향, 전망 등에 대한 전반적인 자료를 파악할 수 있고, 둘째, 정부는 정보보호산업 육성을 위한 방향을 설정할 수 있고, 보다 실천적인 과제를 도출할 수 있을 것이다. 셋째, 본 연구 결과는 정보보호 관련 학계, 연구계의 기초 자료로 활용될 수 있을 뿐만 아니라, 연관 산업 및 관련 기업의 비전과 전략을 설정하는데 있어 기본 자료가 될 수 있을 것이다.

1 Title

2019 Survey of Information Security Industry in Korea

2 Purpose of the Study

The purpose of this study is to investigate the market size and the outlook of domestic Information Security Industry, based on the market survey on Information Security Industry 2019. Furthermore, the study is designed to suggest the policy directions that can lead to the growth of the Information Security Industry in Korea.

3 Contents and Scope

The main contents and scope of this study include general corporate characteristics, current status and the outlook of sales, exports, employment, R&D and their requests for the government support.

4 Results of the Study

○ Business Status of the Information Security Industry

The study found out that there are 1,094 domestic information security businesses, which are comprised of 473 Cyber Security companies and 621 Physical Security ones.

[Table] Number of Domestic Information Security Industry Companies (Unit : EA)

Year	Cyber Security	Physical security	Total
2019	473	621	1,094
2018	464	549	1,013
2017	332	565	897
2016	311	553	864

○ Sales and Outlook of the Information Security Industry

In 2019, the total sales in the Information Security Industry amounted to 10,557,237 million KRW, which was a 4.3 percent increase compared to the previous year. The sales in the Cyber Security reached 3,277,687 million KRW, with a 6.3 percent rise from 3,082,926 million KRW in the previous year. The physical security saw 7,279,550 million KRW in sales, which was a 3.5 percent growth compared to 7,034,918 million KRW in 2018.

[Table] Sales in the Information Security Industry

	Cyber Security			Physical Security			Total		
	2017	2018	2019(E)	2017	2018	2019(E)	2017	2018	2019(E)
Sales (million KRW)	2,744,940	3,082,926	3,277,687	6,840,822	7,034,918	7,279,550	9,585,762	10,117,844	10,557,237
Growth rate (%)	12.3		6.3	2.8		3.5	5.6		4.3

○ Exports and Outlook of the Information Security Industry

The export of Information Security Industry is projected to rise by 5.8 percent, to 1,646,313 million KRW(2019) from 1,556,132 million KRW(2018). The Cyber Security export grew by 31.8 percent, to 108,528 million KRW(2019) from 82,363 million KRW(2018), while the export of physical security increased by 4.3 percent, to 1,537,785 million KRW(2019) from 1,537,785 million KRW(2018).

[Table] Exports in the Information Security Industry

	Cyber Security			Physical Security			Total		
	2017	2018	2019(E)	2017	2018	2019(E)	2017	2018	2019(E)
Export (Million KRW)	94,398	82,363	108,528	1,475,755	1,473,769	1,537,785	1,570,153	1,556,132	1,646,313
Growth rate(%)	-12.7	31.8		-0.1	4.3		-0.9	5.8	

○ Employment in the Information Security Industry

The number of the employed in the Information Security Industry was 46,275 as of December 2018. 13,378 people were employed in Cyber Security businesses, while 32,897 people were employed in physical security companies.

[Table] Employment status in the Information Security Industry (As of December 2018)

	Cyber Security	Physical Security	Classification					
			Less than 4 years	4~7 years	7~11 years	11~15 years	15 or more years	Total
No. of the Employed	13,378	32,897	13,748	12,334	10,438	6,268	3,487	46,275
Percentage (%)	28.9	71.1	29.7	26.7	22.6	13.5	7.5	100.0

The number of new employees in Information Security companies was 4,658 in 2019, and the number is expected to go slightly down to 4,121 in 2020.

Abstract

[Table] Current and expected employment in the Information Security Industry

	2019			2020 (Expected)		
	Cyber Security	Physical security	Total	Cyber Security	Physical security	Total
Number of the employed	1,806	2,852	4,658	1,334	2,787	4,121
Percentage (%)	38.8	61.2	100.0	32.4	67.6	100.0

○ R&D status in the Information Security Industry

As for the possession of intellectual property in the Information Security Industry, the Information Security businesses own 7,093 intellectual property rights and 770 pending intellectual property rights.

[Table] Possession of Intellectual Property

(Unit : Number)

	Owned (Patent Grant)	Request Pending (Patent application)
Cyber Security	2,120	426
Physical Security	4,973	344
Total	7,093	770

○ Demands for Government Support for the Information Security Industry

Government supports such as increased funding and tax benefits is required to revitalize the cyber security industry. Also, creating bigger demands for the public sector is a critical factor for the industry. In the field of physical security, technology development support, funding and tax benefits are more urgently needed.

[Table] Government Support Demanded for Market Growth (multiple response)

(Unit : %)

Demands	Cyber Security	Physical Security
Fostering professional workforce	18.9	7.1
Technical development support	34.1	28.0
The activation of the transfer of technology	6.8	6.2
Amendment of legal systems & regulations	6.5	11.8
Creating Market Demand for the Public Sector	10.8	9.5
Promote consumer investment	4.3	6.6
Funding and tax benefits	15.8	27.5
Expansion of overseas support projects	2.2	2.4
Others	0.6	0.9

○ Policy Implications

The number of companies in the information security industry increased by 8.0% from 1013 in 2018 to 1094 in 2019. This means that business opportunities are increasing in the field of information security, implying that companies are increasing their participation in the industry and the market is growing.

The growth rate of the information security industry showed 6.0% in 2017 and 5.6% in 2018, and 4.3% in 2019, which indicates steady growth in the industry every year. This trend is expected to lead to 10 trillion won of the market size by 2018. The continued growth of the information security market is seems to be due to strengthening of the regulations related to the cyber security industry, heightened awareness and perception of cyber security, strengthened investment in security from both the government and corporations.

The growth of the information security sector in 2019 showed that the product market grew 7.01% and the service market increased 6.32%. In the future, security consulting, maintenance / security management services, and

security monitoring market are expected to grow steadily due to the expansion of ISMS mandates.

One of the biggest difficulties the Korean Information Security Industry is faced with is their entry to overseas market. Many companies are having trouble discovering appropriate business channels in other countries as well as understanding local industrial trends, laws and regulations. Therefore, in order to enhance the international competitiveness of the information security industry, the government should assist the companies with their overseas marketing activities by helping them participate in security exhibitions, connect with foreign public institutions, and publishing a guide book about overseas laws and regulations pertinent to the security world.

In the field of information-oriented security, more financial support tax benefits and public sector market demand growth are needed. Regarding physical security, technology development support, funding and tax benefits are more urgently needed. Therefore, at the government level, it is necessary to consider support for market expansion, technological competitiveness, and funding.

5 Expected Effects

This study presents the following expected effects. First, this study identifies the far-ranging information on the Information Security Industry including industry characteristics, sales, exports, employment status, market trends and the outlook. Second, this study provides the government with a set of guidelines on which the policy directions for the development of the Information Security Industry can be based. Lastly, the result of this study not only can be used as preliminary data by the information security academia, but also can be used to develop visions and strategies for the industry and related companies.

목 차

제1장 조사 개요

1. 조사 목적	3
2. 조사 연혁	3
3. 조사 내용 및 범위	4
4. 조사 체계	5
5. 표본설계	5
6. 실사	5
7. 자료 입력 및 처리	6
8. 결과발표	7
9. 모집단 현황	7

제2장 정보보호산업 개요

1. 정보보호산업의 정의	11
2. 정보보호산업의 특성	13
3. 정보보호산업의 분류	14

제3장 정보보호산업 현황

제1절 기업 현황	19
1. 지역별 현황	19
2. 기업 형태별 현황	21
3. 상장 유무별 현황	21
4. 설립연도별 현황	22
5. 자본금 규모별 현황	22
6. 종사자 규모별 현황	23
제2절 매출 현황	24
1. 매출 현황	24

제3장 정보보호산업 현황

제3절 수출 현황	26
제4절 인력 및 채용 현황	28
1. 인력 현황	28
2. 특성별 현황	30
3. 채용 현황	32
4. 채용 계획	33
제5절 기술개발 및 동향	35

제4장 정보보안산업 현황

제1절 기업 현황	39
1. 지역별 현황	39
2. 기업 형태별 현황	40
3. 상장 유무별 현황	40
4. 설립연도별 현황	41
5. 자본금 규모별 현황	41
6. 종사자 규모별 현황	42
7. 취급 품목별 현황	42
제2절 매출 현황	44
1. 전체 매출 현황	44
2. 특성별 매출 현황	46
3. 제품별 매출 현황	47
4. 서비스별 매출 현황	52
제3절 수출 현황	57
1. 정보보안 시스템 개발 및 공급 수출 현황	59
2. 정보보안 관련 서비스 수출현황	64

제4장 정보보안산업 현황

제4절 인력 및 채용 현황 67

1. 인력 현황 67
2. 특성별 현황 68
3. 채용 현황 73
4. 채용 계획 75

제5절 기술개발 및 동향 76

1. 자체기술연구소 및 연구개발 전담부서 운영 76
2. 연도별 기술개발 투자액 현황 77
3. 기술개발 시 애로사항 78
4. 지식재산권 보유 현황 78
5. 매출 규모별 제품 비중 79
6. 사업추진에 따른 하도급, 유지보수 및 라이선스 요율 정도 80
7. 주요 경쟁 요소 80
8. 기업 경영/기술정보 수집 경로 81
9. 시장 경쟁 및 산업 동향 동의 수준 82
10. 시장 확대를 위한 정부지원 필요 부분 83
11. 해외 진출 시 애로사항 84

제5장 물리보안산업 현황

제1절 기업 현황 87

1. 지역별 현황 87
2. 기업 형태별 현황 88
3. 상장 유무 현황 88
4. 설립연도별 현황 89
5. 자본금 규모별 현황 89
6. 종사자 규모별 현황 90
7. 취급 품목별 현황 90

제5장 물리보안산업 현황

제2절 매출 현황 92

1. 전체 매출 현황 92
2. 특성별 매출 현황 95
3. 제품별 매출 현황 96
4. 서비스별 매출 현황 105

제3절 수출 현황 108

1. 제품별 수출 현황 109

제4절 인력 및 채용 현황 118

1. 인력 현황 118
2. 특성별 현황 119
3. 채용 현황 123
4. 채용 계획 125

제5절 기술개발 및 동향 126

1. 자체기술연구소 및 연구개발 전담부서 운영 126
2. 연도별 기술개발 투자액 현황 127
3. 기술개발 시 애로사항 128
4. 지식재산권 보유 현황 128
5. 매출 규모별 제품 비중 129
6. 주요 경쟁 요소 130
7. 기업 경영/기술정보 수집 경로 131
8. 시장 경쟁 및 산업 동향 동의 수준 132
9. 시장확대를 위한 정부지원 필요 부분 133
10. 해외 진출 시 애로사항 134

제6장 정책적 시사점

1. 정보보호 기업체 수의 증가	137
2. 정보보호산업의 성장세 지속	138
3. 정보보안 분야의 서비스 시장 성장 강세	139
4. 정보보안산업의 수출 규모 크게 성장	140
5. 정보보호 기업의 일자리 창출	141

참고문헌	142
------------	-----

부 록

부 록 1	149
부 록 2	164
부 록 3	183

별 첨

인공지능 기반의 보안기술 동향 및 고려사항	189
양자암호통신과 보안의 미래	204
5G 시대의 위협과 보안	215
융합보안의 현황과 미래전망	225
얼굴인식시스템 동향 및 전망	237

표 목 차

[표 1-1] 국내 정보보호산업 모집단 현황	8
[표 1-2] 국내 정보보호산업 모집단 일반 현황	8
[표 2-1] 2019년 정보보안 제품 및 서비스 분류	15
[표 2-2] 2019년 물리보안 제품 및 서비스 분류	15
[표 3-1] 정보보호 기업 지역별 현황	19
[표 3-2] 정보보호 기업의 지역별 분포	20
[표 3-3] 정보보호 기업 형태별 현황	21
[표 3-4] 정보보호 기업 상장 유무별 현황	21
[표 3-5] 정보보호 기업 설립연도별 현황	22
[표 3-6] 정보보호 기업 자본금 규모별 현황	22
[표 3-7] 정보보호 기업 종사자 규모별 현황	23
[표 3-8] 정보보호산업 매출 현황	24
[표 3-9] 정보보호산업 매출 추이	24
[표 3-10] 정보보안산업 중분류 매출 현황	25
[표 3-11] 물리보안산업 중분류 매출 현황	26
[표 3-12] 정보보호산업 수출 현황	26
[표 3-13] 정보보호산업 국가별 수출 현황	27
[표 3-14] 정보보호산업 수출 추이	27
[표 3-15] 정보보호산업 인력 현황	28
[표 3-16] 정보보호산업 구분별 인력 현황	29
[표 3-17] 정보보호산업 수준별 인력 현황	30
[표 3-18] 정보보호산업 매출액 규모별 인력 현황	30
[표 3-19] 정보보호산업 종사자 규모별 인력 현황	31
[표 3-20] 정보보호산업 기업 형태별 인력 현황	31
[표 3-21] 정보보호산업 채용 현황	32
[표 3-22] 정보보호산업 매출액 규모별 채용 현황	32
[표 3-23] 정보보호산업 종사자 규모별 채용 현황	33
[표 3-24] 정보보호산업 기업 형태별 채용 현황	33
[표 3-25] 정보보호산업 채용 계획	33
[표 3-26] 정보보호 기업 특성별 채용 계획	34
[표 3-27] 기술개발시 애로사항	35
[표 3-28] 지식재산권 보유 현황	36

[표 3-29] 시장 확대를 위한 정부 지원 필요 사항	36
[표 4-1] 정보보안 기업의 지역별 분포	39
[표 4-2] 정보보안 기업 형태별 현황	40
[표 4-3] 정보보안 기업 상장 유무별 현황	40
[표 4-4] 정보보안 기업 설립연도별 현황	41
[표 4-5] 정보보안 기업 자본금 규모별 현황	41
[표 4-6] 정보보안 기업 종사자 규모별 현황	42
[표 4-7] 정보보안 기업의 중분류 품목별 취급 기업 현황	43
[표 4-8] 정보보안산업 대분류 매출 현황	44
[표 4-9] 정보보안산업 중분류 매출 현황	45
[표 4-10] 정보보안산업 업종별(수요처별) 매출 현황	45
[표 4-11] 정보보안산업 특성별 매출 현황	46
[표 4-12] 정보보안 대분류별 수출 현황	57
[표 4-13] 정보보안 제품 및 서비스 수출 현황	57
[표 4-14] 정보보안 국가별 수출 현황	58
[표 4-15] 정보보안산업 구분별 인력 현황	67
[표 4-16] 정보보안산업 인력 현황	68
[표 4-17] 정보보안산업 직종별 인력 현황	69
[표 4-18] 정보보안산업 매출액 규모별 인력 현황	70
[표 4-19] 정보보안산업 종사자 규모별 인력 현황	71
[표 4-20] 정보보안산업 기업 형태별 인력 현황	72
[표 4-21] 정보보안산업 분야별 인력 채용 현황	73
[표 4-22] 정보보안 매출액 규모별 인력 채용 현황	73
[표 4-23] 정보보안 종사자 규모별 인력채용 현황	74
[표 4-24] 정보보안 기업형태별 인력채용 현황	74
[표 4-25] 정보보안산업 분야별 채용계획	75
[표 4-26] 정보보안 기업 특성별 채용 계획	75
[표 4-27] 정보보안 기업 자체기술연구소 및 전담부서 운영 현황	76
[표 4-28] 정보보안 기업 연도별 기술개발 투자액 현황	77
[표 4-29] 정보보안 기술개발시 애로사항	78
[표 4-30] 정보보안 지식재산권 보유 현황	79
[표 4-31] 정보보안 해외특허 보유 현황	79

표 목 차

[표 4-32]	정보보안 매출규모별 제품비중	79
[표 4-33]	사업추진에 따른 하도급, 유지보수 및 라이선스 요율	80
[표 4-34]	정보보안 주요 경쟁 요소	80
[표 4-35]	정보보안 경영/기술정보 수집 경로	81
[표 4-36]	정보보안 시장 경쟁 및 산업 동향 동의 수준	82
[표 4-37]	정보보안 시장 확대를 위한 정부 지원 필요 사항	83
[표 4-38]	정보보안산업 해외 진출시 애로사항	84
[표 5-1]	물리보안 기업의 지역별 분포	87
[표 5-2]	물리보안 기업 형태별 현황	88
[표 5-3]	물리보안 기업 상장 유무별 현황	88
[표 5-4]	물리보안 기업 설립연도별 현황	89
[표 5-5]	물리보안 기업 자본금 규모별 현황	89
[표 5-6]	물리보안 기업 종사자 규모별 현황	90
[표 5-7]	물리보안 기업 중분류 품목별 취급 기업 현황	91
[표 5-8]	물리보안산업 대분류 매출 현황	92
[표 5-9]	물리보안산업 중분류 매출 현황	93
[표 5-10]	물리보안산업 업종별(수요처별) 매출 현황	94
[표 5-11]	기업 특성별 2019년 물리보안산업 매출 현황	95
[표 5-12]	물리보안 제품 수출 현황	108
[표 5-13]	물리보안 국가별 수출 현황	108
[표 5-14]	물리보안산업 구분별 인력 현황	118
[표 5-15]	물리보안산업 특성별 및 직종별 인력 현황	119
[표 5-16]	물리보안산업 매출액 규모별 인력 현황	120
[표 5-17]	물리보안산업 종사자 규모별 인력 현황	121
[표 5-18]	물리보안산업 기업 형태별 인력 현황	122
[표 5-19]	물리보안산업 인력 채용 현황	123
[표 5-20]	물리보안 매출액 규모별 인력 채용 현황	123
[표 5-21]	물리보안 종사자 규모별 인력 채용 현황	124
[표 5-22]	기업 형태별 인력 채용 현황	124
[표 5-23]	물리보안산업 분야별 채용 계획	125
[표 5-24]	물리보안 기업 특성별 채용 계획	125
[표 5-25]	물리보안 자체기술연구소 및 전담부서 운영 현황	126

[표 5-26] 물리보안 기업 연도별 기술개발 투자액 현황	127
[표 5-27] 물리보안 기술개발시 애로사항	128
[표 5-28] 물리보안 지식재산권 보유 현황	129
[표 5-29] 물리보안 해외특허 보유 현황	129
[표 5-30] 물리보안 매출규모별 제품비중	129
[표 5-31] 물리보안 주요 경쟁 요소	130
[표 5-32] 물리보안 경영/기술정보 수집 경로	131
[표 5-33] 물리보안 시장 경쟁 및 산업 동향 동의 수준	132
[표 5-34] 물리보안 시장 확대를 위한 정부 지원 필요 사항	133
[표 5-35] 물리보안산업 해외 진출시 애로사항	134
[표 6-1] 정보보호 기업 종사자 규모 변화	137
[표 6-2] 정보보호산업 매출과 성장률 추이	138
[표 6-3] 정보보안산업 중분류 매출 증감 현황	139
[표 6-4] 정보보호산업 연평균 수출 성장률	140
[표 6-5] 정보보호기업 인력현황	141
[표 6-6] '19년 신규채용 현황 및 '20년 계획	141

그림 목 차

[그림 2-1] 정보보호산업 범위	12
[그림 3-1] 자체기술연구소 및 연구개발 전담부서 운영 현황	35
[그림 4-1] 정보보안기업의 중분류 품목별 취급 기업 현황	43
[그림 4-2] 네트워크 보안 시스템 개발 매출 현황	47
[그림 4-3] 시스템 보안 솔루션 개발 매출 현황	48
[그림 4-4] 정보유출방지 시스템 개발 매출 현황	49
[그림 4-5] 암호/인증 시스템 개발 매출 현황	50
[그림 4-6] 보안관리 시스템 매출 현황	51
[그림 4-7] 보안컨설팅 서비스 매출 현황	52
[그림 4-8] 보안시스템 유지관리/보안성 지속 서비스 매출 현황	53
[그림 4-9] 보안관제 서비스 매출 현황	54
[그림 4-10] 보안교육 및 훈련 서비스 매출 현황	55
[그림 4-11] 공인/사설 인증서 매출 현황	56
[그림 4-12] 네트워크보안 시스템 개발 수출 현황	59
[그림 4-13] 시스템보안 솔루션 개발 수출 현황	60
[그림 4-14] 정보유출방지 시스템 개발 수출 현황	61
[그림 4-15] 암호/인증 시스템 개발 수출 현황	62
[그림 4-16] 보안관리 시스템 개발 수출 현황	63
[그림 4-17] 보안컨설팅 서비스 수출 현황	64
[그림 4-18] 보안시스템 유지관리/보안성 지속 서비스 수출 현황	65
[그림 4-19] 보안관제 서비스 수출 현황	66
[그림 5-1] 물리보안 기업 중분류 품목별 취급 기업 현황	91
[그림 5-2] 보안용 카메라 제조 매출 현황	96
[그림 5-3] 보안용 저장장치 제조 매출 현황	97
[그림 5-4] CCTV 카메라 부품 매출 현황	98
[그림 5-5] 물리보안 솔루션 매출 현황	99
[그림 5-6] 물리보안 주변장비 제조 매출 현황	100
[그림 5-7] 출입통제 장비 제조 매출 현황	101
[그림 5-8] 생체인식 보안 시스템 제조 매출 현황	102
[그림 5-9] 경보/감시 장비 제조 매출 현황	103
[그림 5-10] 기타 제품 매출 현황	104
[그림 5-11] 출동보안서비스 매출 현황	105

[그림 5-12] 영상보안서비스 매출 현황	106
[그림 5-13] 기타보안서비스 매출 현황	107
[그림 5-14] 보안용 카메라 제조 제품 수출 현황	109
[그림 5-15] 보안용 저장장치 제조 수출 현황	110
[그림 5-16] CCTV 카메라 부품 수출 현황	111
[그림 5-17] 물리보안 솔루션 수출 현황	112
[그림 5-18] 물리보안 주변장비 수출 현황	113
[그림 5-19] 출입통제장비 제조 수출 현황	114
[그림 5-20] 생체인식 보안시스템 수출 현황	115
[그림 5-21] 경보/감시 장비 제품 수출 현황	116
[그림 5-22] 기타 제품 수출 현황	117

2019

국내 정보보호산업
실태조사



제1장 조사 개요

1	조사 목적	3
2	조사 연혁	3
3	조사 내용 및 범위	4
4	조사 체계	5
5	표본설계	5
6	실사	5
7	자료 입력 및 처리	6
8	결과발표	7
9	모집단 현황	7

1장

조사 개요

1 조사 목적

본 연구는 2019년 정보보호산업의 시장조사를 통해 산업동향을 파악하고 향후 전망을 예측하는 것을 주된 목적으로 하고 있으며, 나아가 정보보호산업을 육성할 수 있는 정책방향과 과제를 제시하는데 있다.

본 조사의 주요 목적은 다음과 같다.

- ▷ 학계 및 연구계 등에서 정보보호 분야 또는 산업에 대하여 연구를 추진함에 있어 산업과 시장을 이해할 수 있는 기초자료 수집
- ▷ 정보보호산업에 대한 정부의 정책 입안 근거 및 정책 효율 점검용 기본 통계 자료로 활용
- ▷ 정부부처 및 주요 공공기관 등에 보고서를 배포하여 정보보호 산업현황, 인지도 확산 및 국내 정보보호 기업 현황에 대한 자료 제공으로 시장수요 창출
- ▷ 치열한 경쟁 속에서 생존하기 위해 경영전략 수립을 해야 하는 산업체에서 전년도 매출실적과 인력현황, 시장현황 등을 근거로 한 정보보호산업 현황 파악 및 정책방향 설정을 위해 참고자료로 활용

2 조사 연혁

- ▷ 2001년 「국내 정보보호산업 및 실태조사」 최초 조사 시행
- ▷ 2004년 「국내 정보보호산업 통계조사」로 조사명 변경
- ▷ 2007년 「국내 정보보호산업 시장 및 동향조사」로 정보보호산업의 정책적 육성 과제를 도출하고자 조사명 변경

- ▷ 2009년 「국내 지식정보보안산업 시장 및 동향조사」로 조사명 변경
 - 정보보호산업을 ‘정보보안산업, 물리보안산업, 융합보안산업’으로 확대하여 지식정보보안산업으로 전환
- ▷ 2010년 「국내 정보보안산업 실태조사」로 조사명 변경
- ▷ 2011년 「국내 정보보안산업 실태조사」로 조사 실시
- ▷ 2012년 「국내 지식정보보안산업 실태조사」로 조사명 변경
- ▷ 2013년 「국내 정보보호산업 실태조사」로 조사명 변경
- ▷ 2016년 「국내 정보보호산업 실태조사」로 조사 실시
- ▷ 2017년 「국내 정보보호산업 실태조사」로 조사 실시
- ▷ 2018년 「국내 정보보호산업 실태조사」로 조사 실시
- ▷ 2019년 「국내 정보보호산업 실태조사」로 조사 실시

3 조사 내용 및 범위

본 조사는 정보보호산업 중 정보·물리보안의 매출현황, 수출 현황, 고용현황, 기술개발 및 경쟁력 등에 대한 조사로, 기존 조사결과를 활용하여 시계열 분석을 통해 시장 추이를 예측할 수 있도록 하였다.

본 조사의 주요 내용은 다음과 같다.

- ▷ 정보·물리보안 제품 및 서비스 산업의 매출현황
- ▷ 정보·물리보안 제품 및 서비스 산업의 수출현황
- ▷ 정보·물리보안 제품 및 서비스 산업의 인력 및 채용현황
- ▷ 정보·물리보안 제품 및 서비스 산업의 기술개발 및 산업동향

4 조사 체계

- ▷ 모집단 : 전국의 정보·물리보안 기업체(1,094개)
- ▷ 조사주기 : 연 1 회
- ▷ 조사 기간 : 2019년 7월 26일 ~ 9월 28일
- ▷ 조사방법 : 면접조사, 이메일조사, 온라인조사 등 병행
- ▷ 조사기관 : 한국정보보호산업협회 (KISIA)

5 표본설계

가. 모집단

- ▷ 목표모집단(Target Population) : 전국의 정보·물리보안 기업체
- ▷ 조사모집단(Survey Population) : 2019년 6월 30일 기준 전국의 정보·물리보안 및 서비스 사업을 영위하는 기업체

나. 표본추출

- ▷ 조사모집단 구축: ICT통합모집단 DB를 추출하여 수집한 기업체 총 1,094개 기업체(정보보안 464개, 물리보안 549개)
- ▷ 표본추출 : 전수층과 표본층으로 구분

6 실사

- ▷ 조사 방법 : 조사회사 면접원 중 소정의 절차에 의해 선발되고 체계적인 교육을 거친 전문면접원에 의한 조사
- ▷ 실사는 전화 컨택 > 조사표 배부 > 회수 > 검증 > 자료처리 단계로 진행
- ▷ 본 조사 실시 : 2019. 7. 26. ~ 9. 28.

- ▷ 검증 및 보완조사(코딩 및 입력 병행) : 2019. 10. 1. ~ 10. 31.

7 자료 입력 및 처리

가. 자료 검증 및 대체

- ▷ 실사 과정에서의 자료 검증
 - 실사 완료된 설문지에 대해 내용 검토 후 이상이 있는 설문지에 대해 전화를 통한 검증 실시
- ▷ 분석 과정에서의 자료 검증
 - 분석 단계에서 특이값이 발견된 기업체에 대해 전화를 통한 검증 실시
- ▷ 무응답 대체
 - 항목 무응답(Item non-response) : 매출액, 종사자 규모를 이용하여 세분류별 추정값 활용.

나. 자료 입력 및 분석

- ▷ 수집된 자료는 부호화 과정을 통해 전산입력
- ▷ 분석단위 : 매출액, 종사자 규모, 기업형태 등
- ▷ 분석방법 : 무응답 처리가 완료된 자료를 이용하여 사후 층화에 의한 총계 추정
- ▷ 모총계의 추정
 - 업종별 규모별 모집단 특성의 총계에 대한 추정량
 - 전체 모집단 총계 $\hat{Y} = Y_{\text{전수층}} + \hat{Y}_{\text{표본층}}$

표본설계 시 모집단을 전수층과 표본층으로 구분하였으므로 모집단 총계는 다음과 같이 추정함.

$$\hat{Y} = \sum_{h=1}^2 N_h \bar{y}_h$$

여기에서

y_{hk} : h 번째 세부 층의 k 번째 표본 사업장에 대한 관찰값

h : 세부 층의 번호 ($h = 1$ (전수층), 2 (표본층))

k : 세부 층의 사업장 번호 ($k = 1, 2, \dots, n_h$)

n_h : h 번째 세부 층에 대한 표본크기

N_h : h 번째 세부 층에 대한 모집단 크기

$n = \sum_{h=1}^2 n_h$: 전체 표본크기

$N = \sum_{h=1}^2 N_h$: 전체 모집단 크기

$\bar{y}_h = \sum_{k=1}^{n_h} y_{hk} / n_h$: h 번째 세부 층의 표본평균

$\hat{p}_h$: h 번째 세부 층의 표본비율

▷ 모비율의 추정

$$\hat{p} = \sum_{h=1}^2 \frac{N_h}{N} \hat{p}_h$$

8 결과발표

▷ 최종결과보고서를 한국정보보호산업협회(KISIA) 홈페이지에 공시함

9 모집단 현황

국내 소재 정보보호산업 관련 조사 모집단은 정보보안 473개, 물리보안 621개로 총 1,094개이다.

[표 1-1] 국내 정보보호산업 모집단 현황

(단위 : 개)

구분	정보보안	물리보안	합계
모집단 수	473	621	1,094

모집단 기업의 일반 현황을 살펴보면 지역은 서울(본사기준)에 47.3%, 자본구성은 비상장사가 90.5%, 일반기업이 59.7%, 종업원 100인 미만 85.1%, 자본금 10억 미만이 70.1%를 차지하고 있는 것으로 조사되었다.

[표 1-2] 국내 정보보호산업 모집단 일반 현황

분류		기업수(개)	비율(%)	분류		기업수(개)	비율(%)
지역	서울	517	47.3	설 립 년 도	2000년 이전	238	21.8
	서울 외	577	52.7		2000년 이후- 2005년 이전	288	26.3
상장 유무	비상장	990	90.5		2005년 이후- 2010년 이전	238	21.8
	코스닥	88	8.0		2010년 이후	330	30.2
	유가증권	7	0.6	종 업 원	20인 미만	519	47.4
	코넥스	9	0.8		20인-100인 미만	412	37.7
기업 형태	일반기업	653	59.7		100인-200인 미만	85	7.8
	벤처기업	441	40.3		200인 이상	78	7.1
				자 본 금	10억 미만	767	70.1
					10억-50억 미만	239	21.8
					50억-100억 미만	54	4.9
					100억 이상	34	3.1

2019

국내 정보보호산업
실태조사



제2장

정보보호산업 개요

1	정보보호산업의 정의	11
2	정보보호산업의 특성	13
3	정보보호산업의 분류	14

2장 정보보호산업 개요

1 정보보호산업의 정의

정부는 제1차 정보보호산업 진흥계획(K-ICT 시큐리티 2020)을 수립·발표하면서 창업활성화를 통한 글로벌경쟁력 강화, 투자확대 및 신시장 창출, 내수위주에서 글로벌 진출로 시장확대, 지속성장 생태계 조성 등을 중점 추진키로 하였다.

정보보호산업 경쟁력 강화를 위한 10대 정책과제로 △글로벌 스타트업 창업 활성화 △차세대 핵심기술 및 산업형 보안인재 확보 △투자확대 및 산업체질 개선 △융합보안 내재화를 위한 지원체계 구축 및 시장확대 △물리보안 및 차세대 전자인증산업 육성 △정보보호사업의 글로벌스탠다드화 △K-Security 브랜드화 △전략거점 활용 신규시장 확대 △국가사이버 침해대응 역량 강화 △정보보호 협업 거버넌스 강화 및 법제도 개선 등을 선정하여 2020년까지 중점적으로 추진해나가기로 하였다.

이처럼 정부가 적극 나서기로 한 정보보호산업은 초연결사회가 도래함에 따라 사물인터넷(IoT)이 미래의 새로운 경쟁성장 동력으로 부상하고 있는 가운데 향후 우리나라의 미래를 좌우할 최첨단 기술집약적 산업이다. 사실 국내에 정보보호 관련 기업들이 본격적으로 설립된 것은 1990년 중반으로 다른 국가 기간산업에 비해 월등히 역사가 짧다고 할 수 있다.

그럼에도 그동안 우리나라의 정보보호산업은 비약적인 발전을 통해 경쟁력도 확보했으며 수출도 매년 증가하고 있다. 전체 IT 산업에서 차지하는 비중 역시 향후 첨단기술의 발달과 함께 급증할 것으로 예상된다.

2015년 제정된 정보보호산업법 제2조에서는 정보보호산업을 ‘정보보호를 위한 기술 및 정보보호기술이 적용된 제품을 개발·생산 또는 유통하거나 이에 관련한 서비스를 제공하는 산업’으로 정의하였다.

본 보고서에서는 정보보안과 물리보안 분야를 포함한 정보보호산업의 공급자 중심

기업을 대상으로 일반적 특성, 매출현황 및 전망, 수출현황, 인력 및 고용현황, 기술개발 현황을 주요 내용으로 하였다.

[그림 2-1] 정보보호산업 범위

정보보안	물리보안	융합보안
		
해킹/침입탐지, 개인정보유출방지 컴퓨터포렌식 등	영상감시, 바이오인식, 무인전자경비 등	운송보안(자동차/항공 등) /의료/건설/국방 보안 방법보안로봇 등
정보보안(클린인터넷경제)	물리보안(안전안심생활)	융합보안(안전성강화)

정보보호산업은 정보보호제품을 개발·생산 또는 유통하거나 정보보호에 관한 컨설팅, 보안관제 등 서비스를 수행하는 산업으로서 기술의 적용영역, 제품의 특성 등에 따라 정보보안, 물리보안, 융합보안(정보보안+물리보안, 정보보안+他산업)으로 분류된다. 이는 크게 컴퓨터 또는 네트워크상 정보 유출·훼손 등을 방지하기 위한 정보보안, 재난·재해, 범죄 등을 방지하기 위한 물리보안, 자동차나 항공해상 보안 등의 융합보안으로 구분된다. 북미, 유럽, 일본 등 주요 선진국이 정보보호 시장의 90% 가량 차지하고 있으며, 최근에는 중국이라는 새로운 보안 시장이 대두되고 있다.

전 세계 정보보호산업 시장 규모는 향후 해마다 증가할 것으로 예상되는데, 이는 기존 인터넷 및 스마트폰 이용부터 융합보안과 새롭게 떠오르고 있는 IoT(사물인터넷)의 등장으로 보안의 중요성이 커지고 있기 때문이다.

2 정보보호산업의 특성

정보보호산업의 특징은 다음과 같다. “창과 방패”처럼, 진화하는 보안위협에 대응하여 지속적인 R&D가 필요한 분야이며, 보안위협의 대응과 우수한 제품 개발을 위해서는 암호·인증·인식·감시 등의 보안 분야 학문 외에 인문학·공학 등 다학제적인 연구 및 인재가 필요한 분야이다.

또한 보안사고 발생시 개인·사회·국가 등 전 영역에 영향을 주는 등 파급력이 매우 크고 최근 전 산업의 IT화로 대부분의 산업에 보안기술 적용이 요구되고 있으며, 평상시에는 중요성을 인식 못하지만 사고 발생시에는 높은 수준의 품질을 요구하게 되는 특징을 가지고 있다.

우리나라의 정보보호의 자주성을 확보하고 국가의 중요정보 유출을 미연에 방지하기 위해서는 무엇보다 국내 정보보호업체의 기술수준을 향상시키고 이를 활용하는 것이 필요하다고 할 수 있다. 특히 정보보호산업은 다음과 같은 특성이 있다.

① 성장발전 가능성이 높은 신성장 산업

첫째, 정보보호산업은 성장발전 가능성이 높은 신성장 산업으로, 시스템·네트워크 보안 중심의 정보보안과 CCTV·저장장치·무인경비서비스 등의 물리보안, 타 산업 군에 보안기술이 적용되는 활용분야(융합보안)로 구분된다. 향후 지능화된 보안위협 및 자동차·안전 등 타 분야의 신규 보안이슈의 확대로 시장은 더 커질 것으로 전망된다.

본 보고서에서는 활용분야(융합보안)가 아직 성장단계임을 감안하여 산업 규모 파악에서 제외하였으며, 정보·물리보안의 규모를 파악하는 것에 일차적인 목표를 두었다.

정보·물리보안은 크게 시스템 개발 및 공급(제품)과 관련 서비스 산업으로 분리하였으며, 정보보안 시스템 개발 및 공급 산업은 ‘네트워크보안 시스템 개발’, ‘시스템보안 솔루션 개발’, ‘정보유출방지 시스템 개발’, ‘암호/인증 시스템 개발’, ‘보안관리 시스템 개발’ 등 5개 시스템 개발 및 공급군으로 크게 분리하였고, 정보보안 관련 서비스 산업은 ‘보안컨설팅 서비스’, ‘보안시스템 유지관리/보안성 지속 서비스’, ‘보안관제 서비스’, ‘보안교육 및 훈련 서비스’, ‘공인/사설 인증서’ 등 5개 서비스군으로 분리하였다. 또한, 물리보안 시스템 개발 및 공급(제품)은 ‘보안용 카메라 제조’, ‘보안용 저장장치 제조’, ‘CCTV 카메라 부품’, ‘물리보안 솔루션’, ‘물리보안 주변장비’, ‘출입통제 장비 제

조’, ‘생체인식 보안시스템 제조’, ‘경보/감시 장비 제조’, ‘기타 제품’ 등 9개 시스템 개발 및 공급군으로 분리하였으며, 물리보안 관련 서비스 산업을 ‘출동보안 서비스’, ‘영상보안 서비스’, ‘기타보안 서비스’ 등 3개 서비스 군으로 분리하였다.

② 국가의 안보와 관련된 방위 산업

둘째, 정보보호산업은 국가의 안위를 지켜주는 방위산업이다. 협의의 개념으로는 개인의 안전과 재산을 지켜주는 보안산업이고, 광의의 개념으로는 각종 테러와 보이지 않는 전쟁(사이버테러 및 정보화 전쟁)으로부터 국가의 안위를 지켜주는 방위산업이다.

정보보호산업은 밖으로는 금융기관의 IT보안 서비스, 국제범죄, 국제해커로 부터의 침입차단 등 국가를 위협으로부터 지켜주고, 안으로는 주정차 차량 감시 CCTV 등을 활용하여 질서 확립 및 각종 범죄 예방 및 치안을 담당하므로 방위산업이라 할 수 있다.

③ 차세대 고부가가치 미래지향 산업

셋째, 정보보호산업은 미래지향 산업이다. 최근 국내 IT 산업은 스마트폰, 태블릿 PC 등 스마트 모바일 기기 시장 뿐만 아니라 IoT(사물인터넷) 및 클라우드 컴퓨팅 등 큰 변화가 있어왔다. 이에 정보보안 및 무선통신망의 안전성 강화에 대응해야 할 것이며, IT산업을 기반으로 한 미래 생활에 정보보호산업 기술이 포함되어 응용되고 있다.

3 정보보호산업의 분류

정보보호산업의 특성상 제품과 서비스의 통합화 및 융합화가 매우 빠르게 진행되고 있어 정보보호산업을 분류할 때, 예전의 하드웨어, 소프트웨어, 서비스의 3분야의 구분이 점차 모호해지고 있다.

이에 본 조사는 설문조사에 들어가기에 앞서 정보보호산업 관련 학계, 산업계 등 전문가로부터 산업품목에 대한 심도 깊은 조사를 실시하여 자체적으로 정보보호산업 분류를 구성하였다.

앞서 언급한 내용과 같이 정보보호산업은 정보보안과 물리보안으로 크게 구분할 수 있으며, 각각의 구체적 분류는 [표 2-1] 및 [표 2-2]와 같다.

[표 2-1] 2019년 정보보안 제품 및 서비스 분류

대분류	소분류
정보보안 시스템 개발 및 공급	네트워크보안 시스템 개발
	시스템보안 솔루션 개발
	정보유출방지 시스템 개발
	암호/인증 시스템 개발
	보안관리 시스템 개발
정보보안 관련 서비스	보안컨설팅 서비스
	보안시스템 유지관리/보안성 지속 서비스
	보안관제 서비스
	보안교육 및 훈련 서비스
	공인/사설 인증서

[표 2-2] 2019년 물리보안 제품 및 서비스 분류

대분류	소분류
물리보안 시스템 개발 및 공급	보안용 카메라 제조
	보안용 저장장치 제조
	CCTV 카메라 부품
	물리보안 솔루션
	물리보안 주변장비
	출입통제 장비 제조
	생체인식 보안시스템 제조
	경보/감시 장비 제조
	기타 제품
물리보안 관련 서비스	출동보안 서비스
	영상보안 서비스
	기타보안 서비스

2019

국내 정보보호산업
실태조사



제3장

정보보호산업 현황

제1절	기업 현황	19
제2절	매출 현황	24
제3절	수출 현황	26
제4절	인력 및 채용 현황	28
제5절	기술개발 및 동향	35

3장

정보보호산업 현황

제1절 기업 현황

1 지역별 현황

정보보호 관련 기업체 소재지를 분석한 결과 1,094개 기업 중 517개(47.3%)가 서울에 위치한 것으로 나타났다. 정보보안 기업은 326개(68.9%), 물리보안 기업은 191개(30.8%)가 서울에 위치한 것으로 나타나 정보보안 기업이 서울에 더 많이 소재한 것으로 조사되었다.

[표 3-1] 정보보호 기업 지역별 현황

(단위 : 개, %)

구분	정보보안		물리보안		합계	
	기업수	비율(%)	기업수	비율(%)	기업수	비율(%)
서울	326	68.9	191	30.8	517	47.3
서울 외	147	31.1	430	69.2	577	52.7
합계	473	100.0	621	100.0	1,094	100.0

정보보안 관련 기업체의 소재지를 분석한 결과 473개 기업 가운데 326개 기업(68.9%)이 서울에 소재하고 있는 것으로 조사되었다. 그 다음으로 경기 53개(11.2%), 대전 27개(5.7%), 부산 13개(2.7%), 대구 9개(1.9%) 순으로 조사되었다. 서울, 경기, 인천 등 수도권에 정보보안 기업의 81.2%가 집중되어 있는 것으로 나타났다.

물리보안 관련 기업 소재지의 경우 621개 기업 가운데 191개 기업(30.8%)이 서울에 소재하고 있는 것으로 조사되었다. 경기 242개(39.0%), 인천 30개(5.8%), 대전 23개(3.7%) 순으로 조사되었다. 서울, 경기, 인천 등 수도권에 물리보안 기업의 74.6%가 집중되어 있는 것으로 나타났다.

[표 3-2] 정보보호 기업의 지역별 분포

(단위 : 개, %)

지역	정보보안		물리보안		합계	
	기업수	비율(%)	기업수	비율(%)	기업수	비율(%)
서울	326	68.9	191	30.8	517	47.3
경기	53	11.2	242	39.0	295	27.0
대전	27	5.7	23	3.7	50	4.6
부산	13	2.7	18	2.9	31	2.8
대구	9	1.9	18	2.9	27	2.5
광주	7	1.5	16	2.6	23	2.1
전남	7	1.5	8	1.3	15	1.4
경남	6	1.3	16	2.6	22	2.0
경북	5	1.1	19	3.1	24	2.2
인천	5	1.1	30	4.8	35	3.2
제주	3	0.6	2	0.3	5	0.5
충남(세종)	3	0.6	7	1.1	10	0.9
충북	3	0.6	5	0.8	8	0.7
강원	2	0.4	10	1.6	12	1.1
울산	2	0.4	5	0.8	7	0.6
전북	2	0.4	11	1.8	13	1.2
합계	473	100.0	621	100.0	1,094	100.0

2 기업 형태별 현황

정보보호 관련 기업체의 기업 형태별 현황을 조사한 결과 일반기업이 653개(59.7%), 벤처기업이 441개(40.3%)인 것으로 나타났다. 정보보안의 경우와 물리보안의 경우 각각 일반기업(65.3%)이 벤처기업(34.7%) 보다, 일반기업(55.4%)이 벤처기업(44.6%)보다 높게 나타났다.

[표 3-3] 정보보호 기업 형태별 현황

(단위 : 개, %)

구분	정보보안		물리보안		합계	
	기업수	비율(%)	기업수	비율(%)	기업수	비율(%)
일반기업	309	65.3	344	55.4	653	59.7
벤처기업	164	34.7	277	44.6	441	40.3
합계	473	100.0	621	100.0	1,094	100.0

3 상장 유무별 현황

정보보호 관련 기업체의 상장¹⁾ 유무별 현황을 조사해보면 비상장 기업이 990개(90.5%), 코스닥 기업이 88개(8.0%), 유가증권시장 기업이 7개(0.6%), 코넥스 기업이 9개(0.8%)인 것으로 조사되었다. 정보보안의 경우 85.4%, 물리보안의 경우 94.4%로 비상장 중소기업이 주를 이루고 있는 것으로 조사되었다.

[표 3-4] 정보보호 기업 상장 유무별 현황

(단위 : 개, %)

구분	정보보안		물리보안		합계	
	기업수	비율(%)	기업수	비율(%)	기업수	비율(%)
비상장	404	85.4	586	94.4	990	90.5
코스닥	57	12.1	31	5.0	88	8.0
유가증권	5	1.0	2	0.3	7	0.6
코넥스	7	1.5	2	0.3	9	0.8
합계	473	100.0	621	100	1,094	100.0

1) 상장회사(상장회사, listed company)란 한국거래소가 정하는 상장심사 기준을 충족시켜 그 발행주식이 시장에서 매매되는 회사를 의미하며, 유가증권시장, 코스닥시장, 코넥스시장 상장회사로 구분된다.

4 설립연도별 현황

정보보호 관련 기업체의 설립연도별 현황을 살펴보면 2000년 이전 설립 기업이 238개(21.8%), 2000년 이후 2005년 이전 설립 기업이 288개(26.3%), 2005년 이후 2010년 이전 설립 기업이 238개(21.8%), 2010년 이후 설립 기업이 330개(30.2%)인 것으로 조사되었다. 2010년 이후부터 신규 설립된 정보보안 기업은 27.1%, 물리보안 기업은 32.5%로 나타났다.

[표 3-5] 정보보호 기업 설립연도별 현황

(단위 : 개, %)

구분	정보보안		물리보안		합계	
	기업수	비율(%)	기업수	비율(%)	기업수	비율(%)
2000년 이전	105	22.2	133	21.4	238	21.8
2000년 이후-2005년 이전	135	28.5	153	24.6	288	26.3
2005년 이후-2010년 이전	105	22.2	133	21.4	238	21.8
2010년 이후	128	27.1	202	32.5	330	30.2
합계	473	100.0	621	100.0	1,094	100.0

5 자본금 규모별 현황

정보보호 관련 기업체의 자본금 규모를 조사한 결과 자본금 10억 미만 기업이 767개(70.1%), 10억 이상 50억 미만 기업이 239개(21.8%), 50억 이상 100억 미만 기업이 54개(4.9%), 100억 이상 기업이 34개(3.1%)인 것으로 조사되었다. 자본금이 50억 미만인 기업은 정보보안 89.4%, 물리보안 93.9%로 대부분을 차지함을 알 수 있다.

[표 3-6] 정보보호 기업 자본금 규모별 현황

(단위 : 개, %)

구분	정보보안		물리보안		합계	
	기업수	비율(%)	기업수	비율(%)	기업수	비율(%)
10억 미만	309	65.3	458	73.8	767	70.1
10억-50억 미만	114	24.1	125	20.1	239	21.8
50억-100억 미만	26	5.5	28	4.5	54	4.9
100억 이상	24	5.0	10	1.6	34	3.1
합계	473	100.0	621	100.0	1,094	100.0

6 종사자 규모별 현황

정보보호 관련 기업체의 종업원 규모별 현황을 살펴보면 20인 미만 기업이 519개(47.4%), 20인 이상 100인 미만 기업이 412개(37.7%), 100인 이상 200인 미만 기업이 85개(7.8%), 200인 이상 기업이 78개(7.1%)인 것으로 조사되었다. 종업원 수가 100인 미만인 기업은 정보보안 80.4%, 물리보안 88.6%로 전체의 85.1%를 차지하고 있음을 알 수 있다.

[표 3-7] 정보보호 기업 종사자 규모별 현황

(단위 : 개, %)

구분	정보보안		물리보안		합계	
	기업수	비율(%)	기업수	비율(%)	기업수	비율(%)
20인 미만	181	38.2	338	54.5	519	47.4
20인~100인 미만	200	42.2	212	34.1	412	37.7
100인~200인 미만	52	11.1	33	5.3	85	7.8
200인 이상	40	8.5	38	6.1	78	7.1
합계	473	100.0	621	100.0	1,094	100.0

제2절 매출 현황

1 매출 현황

2019년 전체 정보보호산업 매출액은 총 10,557,237백만원으로 2018년 대비 4.3% 증가한 것으로 조사되었다. 정보보안 매출액은 2018년 3,082,926백만원에서 2019년 3,277,687백만원으로 6.3% 증가하였으며, 물리보안 매출액은 2018년 7,034,918백만원에서 2019년 7,279,550백만원으로 3.5% 증가하였다.

[표 3-8] 정보보호산업 매출 현황

구분	정보보안			물리보안			합계		
	2017년	2018년	2019년(E)	2017년	2018년	2019년(E)	2017년	2018년	2019년(E)
매출액 (백만원)	2,744,940	3,082,926	3,277,687	6,840,822	7,034,918	7,279,550	9,585,762	10,117,844	10,557,237
성장률 (%)	12.3		6.3	2.8		3.5	5.6		4.3

정보보호산업 매출액은 2013년 7,100,205백만원에서 연평균 6.8%씩 지속적으로 성장하고 있다. 이 중에서 정보보안 매출액은 2013년 1,631,113백만원에서 연평균 12.3%씩 성장하고 있으며, 물리보안 매출액은 2013년 5,469,092백만원에서 연평균 4.9%씩 성장하고 있다. 정보보호산업 매출액이 성장을 지속하고 있는 것은 정부의 법·제도 정비, 최근 보안사고 증가로 인한 경각심 고조, 정부 및 기업의 보안 투자 강화, 해외 진출 노력 등이 주요 원인인 것으로 분석된다.

[표 3-9] 정보보호산업 매출 추이

(단위: 백만원, %)

구분	정보보안	물리보안	합계
2013년	1,631,113	5,469,092	7,100,205
2014년	1,735,865	5,519,452	7,255,317
2015년	2,108,659	6,110,086	8,218,745
2016년	2,454,024	6,588,787	9,042,811
2017년	2,744,940	6,840,822	9,585,762
2018년	3,082,926	7,034,918	10,117,844
2019년(E)	3,277,687	7,279,550	10,557,237
CAGR('13~'19)(%)	12.3	4.9	6.8

가. 정보보안산업 매출 현황

정보보안은 네트워크 보안 시스템 개발(771,656백만원), 시스템보안 솔루션 개발(523,115백만원) 분야의 매출 비중이 높으며, 보안교육 및 훈련 서비스(71.8%) 분야의 증가율이 높은 것으로 조사되었다.

[표 3-10] 정보보안산업 중분류 매출 현황

(단위 : 백만원, %)

구분		2018년	2019년(E)	증감율(%)
정보보안 시스템 개발 및 공급	네트워크보안 시스템 개발	729,393	771,656	5.8
	시스템보안 솔루션 개발	488,402	523,115	7.1
	정보유출방지 시스템 개발	426,128	456,251	7.1
	암호/인증 시스템 개발	151,879	161,760	6.5
	보안관리 시스템 개발	297,920	327,790	10.0
	소계	2,093,723	2,240,572	7.0
정보보안 관련 서비스	보안컨설팅 서비스	302,099	321,478	6.4
	보안시스템 유지관리/ 보안성 지속 서비스	351,942	359,645	2.2
	보안관제 서비스	273,927	286,880	4.7
	보안교육 및 훈련 서비스	1,740	2,990	71.8
	공인/사설 인증서	59,496	66,122	11.1
	소계	989,203	1,037,115	4.8
합계		3,082,926	3,277,687	6.3

정보보안 시스템 개발 및 공급 부문에서는 최근 각종 사이버보안 사고 발생 등에 따라 시스템보안 솔루션 개발, 보안관리 시스템 개발 제품의 수요가 증가한 것으로 분석된다.

정보보안 관련 서비스 부문에서는 보안 공격의 지능화, 고도화, 복잡/다양화에 대응하기 위한 보안교육 및 훈련 서비스가 크게 증가하는 것으로 분석되었다.

나. 물리보안산업 매출 현황

물리보안 제품은 물리보안 솔루션, 생체인식 보안시스템 제조, 기타보안서비스 품목의 증가율이 상대적으로 높게 나타났다. 이는 물리보안 제품의 네트워크화, 지능화 등이 주요 요인으로 분석된다.

[표 3-11] 물리보안산업 중분류 매출 현황

(단위 : 백만원, %)

구분		2018년	2019년(E)	증감율(%)
물리보안 시스템 개발 및 공급	보안용 카메라 제조	1,106,250	1,171,005	5.9
	보안용 저장장치 제조	907,487	923,263	1.7
	CCTV 카메라 부품	484,766	506,379	4.5
	물리보안 솔루션	378,902	419,198	10.6
	물리보안 주변장비	161,576	164,153	1.6
	출입통제 장비 제조	499,455	505,019	1.1
	생체인식 보안시스템 제조	293,378	315,218	7.4
	경보/감시 장비 제조	220,715	221,179	0.2
	기타 제품	369,398	374,307	1.3
	소계	4,421,928	4,599,723	4.0
물리보안 관련 서비스	출동보안서비스	1,726,210	1,727,972	0.1
	영상보안서비스	401,777	415,647	3.5
	기타보안서비스	485,004	536,208	10.6
	소계	2,612,990	2,679,827	2.6
합계		7,034,918	7,279,550	3.5

제3절 수출 현황

정보보호산업 수출액은 2018년 1,570,153백만원에서 2019년에는 5.8% 증가한 1,646,313백만원이 될 것으로 예상된다. 정보보안 수출액은 2018년 82,363백만원에서 2019년 108,528백만원으로 31.8% 증가하였으며, 물리보안 수출액은 2018년 1,473,769백만원에서 2019년 1,537,785백만원으로 4.3% 증가하였다.

[표 3-12] 정보보호산업 수출 현황

구분	정보보안			물리보안			합계		
	2017년	2018년	2019년(E)	2017년	2018년	2019년(E)	2017년	2018년	2019년(E)
수출액 (백만원)	94,398	82,363	108,528	1,475,755	1,473,769	1,537,785	1,570,153	1,556,132	1,646,313
증감율(%)	-12.7		31.8	-0.1		4.3	-0.9		5.8

2018년 기준으로 정보보안의 경우 권역별 수출비중의 49.2% 정도가 일본에서 발생하고 있으며, 물리보안의 경우 권역별 수출비중의 18.8% 정도가 미국에서, 43.7%는 기타 지역에서 발생하는 것으로 나타났다.

[표 3-13] 정보보호산업 국가별 수출 현황

(단위 : %)

구분	정보보안		물리보안	
	2017년	2018년	2017년	2018년
일본	42.4	49.2	11.6	12.6
중국	20.7	18.5	9.0	8.6
미국	14.3	5.6	20.6	18.8
유럽	2.4	1.0	19.2	16.3
기타	20.3	25.7	39.5	43.7

정보보호산업 수출액은 2013년 1,494,456백만원에서 연평균 1.6%씩 성장하고 있다. 이 중에서 정보보안 수출액은 2013년 70,422백만원에서 연평균 7.5%씩 성장하고 있으며, 물리보안 수출액은 2013년 1,424,034백만원에서 연평균 1.3%씩 성장하고 있으나, 2015년 이후 수출액이 감소 및 정체되고 있는 것은 엔화 약세 및 중국제품의 저가 공세 등이 원인으로 분석되고 있다.

[표 3-14] 정보보호산업 수출 추이

(단위: 백만원, %)

구분	정보보안	물리보안	합계
2013년	70,422	1,424,034	1,494,456
2014년	72,989	1,454,461	1,527,450
2015년	78,133	1,545,540	1,623,673
2016년	88,978	1,400,102	1,489,080
2017년	94,398	1,475,755	1,570,153
2018년	82,363	1,473,769	1,556,132
2019년(E)	108,528	1,537,785	1,646,313
CAGR('13-'19)(%)	7.5	1.3	1.6

제4절 인력 및 채용 현황

1 인력 현황

정보보호산업 인력 수는 총 46,275명(2018년 12월 기준)으로, 이 중 정보보안 인력은 28.9%인 13,378명, 물리보안 인력은 71.1%인 32,897명인 것으로 조사되었다. 직급별로는 15년 이상 기술자가 7.5%인 3,487명, 11년 이상 15년 미만 기술자가 13.5%인 6,268명, 7년 이상 11년 미만 기술자가 22.6%인 10,438명, 4년 이상 7년 미만 기술자가 26.7%인 12,334명, 4년 미만 기술자가 29.7%인 13,748명으로 조사되었다.

[표 3-15] 정보보호산업 인력 현황

(2018년 12월 현재)

구분	정보보안	물리보안	합계					
			4년 미만	4년 이상 7년 미만	7년 이상 11년 미만	11년 이상 15년 미만	15년 이상	총합계(명)
인원수(명)	13,378	32,897	13,748	12,334	10,438	6,268	3,487	46,275
비중(%)	28.9	71.1	29.7	26.7	22.6	13.5	7.5	100.0

정보보호담당 인력수는 총 46,275명(2018년 12월 기준)으로, 기업당 평균 42명을 보유하고 있는 것으로 조사되었다. 지역별로 살펴보면 서울 소재기업이 평균 48명으로, 설립연도로는 2000년 이전 설립 기업이 평균 87명으로 보안 인력의 비중이 높은 것으로 조사되었다. 자본금 규모별로 살펴보면 100억 이상 기업이 평균 373명으로 가장 많은 보안인력을 보유하고 있는 것으로 조사되었으며, 종사자수 규모별로 살펴보면 200인 이상 기업이 평균 434명으로 많은 보안인력을 보유하고 있는 것으로 조사되었다. 상장 유무별로 살펴보면 코스닥 기업은 182명, 기업 형태별로 살펴보면 일반기업이 평균 57명의 정보보호 인력을 보유하고 있는 것으로 조사되었다.

[표 3-16] 정보보호산업 구분별 인력 현황

(2018년 12월 현재)

구분		기업수 (개)	정보보호 담당인력(명)		전체 인력(명)		비중(%)
			합계	평균	합계	평균	
전체		1,094	46,275	42	113,402	104	40.8
지역	서울	517	24,881	48	60,511	117	41.1
	서울 외	577	21,394	37	52,891	92	40.4
상장 유무	비상장	990	28,936	29	76,097	77	38.0
	코스닥	88	16,011	182	33,087	376	48.4
	유가증권	7	1,131	162	3,835	548	29.5
	코넥스	9	197	22	383	43	51.4
기업 형태	일반기업	653	37,176	57	94,129	144	39.5
	벤처기업	441	9,099	21	19,273	44	47.2
설립 연도	2000년 이전	238	20,725	87	55,058	231	37.6
	2005년 이전	288	5,830	20	13,139	46	44.4
	2010년 이전	238	12,229	51	28,702	121	42.6
	2010년 이후	330	7,491	23	16,503	50	45.4
종사자	20인 미만	519	1,785	3	4,080	8	43.8
	20인-100인 미만	412	5,936	14	13,742	33	43.2
	100인-200인 미만	85	4,726	56	7,684	90	61.5
	200인 이상	78	33,828	434	87,896	1,127	38.5
자본금	10억 미만	767	5,877	8	15,453	20	38.0
	10억-50억 미만	239	16,020	67	38,813	162	41.3
	50억-100억 미만	54	11,681	216	23,493	435	49.7
	100억 이상	34	12,697	373	35,643	1,048	35.6

2 특성별 현황

정보보호산업 인력은 총 46,275명으로 이 중에서 4년 미만이 13,748명(29.7%), 4년 이상 7년 미만 12,334명(26.7%), 7년 이상 11년 미만 10,438명(22.6%), 11년 이상 15년 미만 6,268명(13.5%), 15년 이상 3,487명(7.5%)인 것으로 조사되었다. 정보 보안 및 물리보안 기업 모두 4년 미만에서 15년 이상 순으로 갈수록 인력 수는 적어지는 특징을 보이는 것으로 나타났다.

[표 3-17] 정보보호산업 수준별 인력 현황

(2018년 12월 현재)

구분	4년 미만	4년 이상 7년 미만	7년 이상 11년 미만	11년 이상 15년 미만	15년 이상	총합계(명)
정보보안	3,837	3,908	2,915	1,825	893	13,378
물리보안	9,911	8,426	7,523	4,443	2,594	32,897
합계	13,748	12,334	10,438	6,268	3,487	46,275
비중(%)	29.7	26.7	22.6	13.5	7.5	100.0

정보보호산업 매출액 규모별 인력 현황을 살펴보면, 100억 이상 기업체가 전체 46,275명 중 39,830명을 보유하고 있으며, 10억 미만 기업체가 929명, 10억 이상 50억 미만 기업체가 2,896명, 50억 이상 100억 미만 기업체가 2,620명의 인력을 보유하고 있는 것으로 조사되었다.

[표 3-18] 정보보호산업 매출액 규모별 인력 현황

(2018년 12월 현재)

매출액 규모	4년 미만	4년 이상 7년 미만	7년 이상 11년 미만	11년 이상 15년 미만	15년 이상	총합계(명)
10억 미만	246	259	208	140	76	929
10억~50억 미만	657	754	734	491	260	2,896
50억~100억 미만	690	820	651	294	165	2,620
100억 이상	12,155	10,501	8,845	5,343	2,986	39,830
합계	13,748	12,334	10,438	6,268	3,487	46,275

정보보호산업 종사자 규모별 인력 현황을 살펴보면 200인 이상 기업체가 33,828명을 보유하고 있으며, 100인 이상 200인 미만 기업체가 4,726명, 20인 이상 100인 미만 기업체가 5,936명, 20인 미만 기업체가 1,785명을 보유하고 있는 것으로 조사되었다.

[표 3-19] 정보보호산업 종사자 규모별 인력 현황

(2018년 12월 현재)

종사자 규모	4년 미만	4년 이상 7년 미만	7년 이상 11년 미만	11년 이상 15년 미만	15년 이상	총합계 (명)
20인 미만	474	514	411	253	133	1,785
20인~100인 미만	1,367	1,545	1,555	976	493	5,936
100인~200인 미만	1,170	1,243	1,216	705	392	4,726
200인 이상	10,737	9,032	7,256	4,334	2,469	33,828
합계	13,748	12,334	10,438	6,268	3,487	46,275

정보보호산업 형태별 인력 현황을 살펴보면 일반기업이 37,176명을 보유하고 있으며, 벤처기업이 9,099명을 보유하고 있는 것으로 조사되었다.

[표 3-20] 정보보호산업 기업 형태별 인력 현황

(2018년 12월 현재)

기업 형태	4년 미만	4년 이상 7년 미만	7년 이상 11년 미만	11년 이상 15년 미만	15년 이상	총합계 (명)
일반기업	11,197	9,977	8,459	4,860	2,683	37,176
벤처기업	2,551	2,357	1,979	1,408	804	9,099
합 계	13,748	12,334	10,438	6,268	3,487	46,275

3 채용 현황

2019년 정보보호 기업체의 신규 채용 현황은 총 4,658명이며, 이 중에서 신입은 1,969명(42.3%), 경력은 2,689(57.7%)로 경력직이 더 많은 것으로 조사되었다.

[표 3-21] 정보보호산업 채용 현황

(2019년 추정)

구분	정보보안			물리보안			합계		
	신입	경력	소계	신입	경력	소계	신입	경력	합계
인원수(명)	803	1,003	1,806	1,166	1,686	2,852	1,969	2,689	4,658
비중(%)	40.9	59.1	100.0	44.5	55.5	100.0	42.3	57.7	100.0

매출액 규모별 2019년 채용 현황을 살펴보면 총 4,658명 중 10억 미만 기업에서의 채용자는 112명(2.4%), 10억 이상 50억 미만 기업의 채용자는 553명(11.9%), 50억 이상 100억 미만 기업의 채용자는 419명(9.0%), 100억 이상 기업의 채용자는 3,574명(76.7%)으로 조사되었다.

[표 3-22] 정보보호산업 매출액 규모별 채용 현황

(2019년 추정)

구분	정보보안		물리보안		합계	
	채용자수(명)	비중(%)	채용자수(명)	비중(%)	채용자수(명)	비중(%)
10억 미만	64	3.5	48	1.7	112	2.4
10억-50억 미만	279	15.4	274	9.6	553	11.9
50억-100억 미만	313	17.3	106	3.7	419	9.0
100억 이상	1,150	63.7	2,424	85.0	3,574	76.7
합계	1,806	100.0	2,852	100.0	4,658	100.0
비중(%)	38.8	-	61.2	-	100.0	-

종사자 규모별 2019년 채용 현황을 살펴보면 총 4,658명 중 20인 미만 기업의 채용자는 275명(5.9%), 20인 이상 100인 미만 기업의 채용자는 850명(18.2%), 100인 이상 200인 미만 기업의 채용자는 581명(12.5%), 200인 이상 기업의 채용자는 2,952명(63.4%)으로 조사되었다.

[표 3-23] 정보보호산업 종사자 규모별 채용 현황

(2019년 추정)

구분	정보보안		물리보안		합계	
	채용자수(명)	비중(%)	채용자수(명)	비중(%)	채용자수(명)	비중(%)
20인 미만	170	9.4	105	3.7	275	5.9
20인-100인 미만	520	28.8	330	11.6	850	18.2
100인-200인 미만	337	18.7	244	8.6	581	12.5
200인 이상	779	43.1	2,173	76.1	2,952	63.4
합계	1,806	100.0	2,852	100.0	4,658	100.0
비중(%)	38.8	-	61.2	-	100.0	-

기업 형태별 2019년 채용 현황을 살펴보면 총 4,658명 중 일반기업의 채용자는 3,450명(74.1%), 벤처기업의 채용자는 1,208명(25.9%)인 것으로 조사되었다.

[표 3-24] 정보보호산업 기업 형태별 채용 현황

(2019년 추정)

구분	정보보안		물리보안		합계	
	채용자수(명)	비중(%)	채용자수(명)	비중(%)	채용자수(명)	비중(%)
일반기업	1,192	66.0	2,258	79.2	3,450	74.1
벤처기업	614	34.0	594	20.8	1,208	25.9
합계	1,806	100.0	2,852	100.0	4,658	100.0
비중(%)	38.8	-	61.2	-	100.0	-

4 채용 계획

2020년 정보보호 기업체의 신규 채용 계획 인원은 총 4,121명으로 이 중에서 신입은 1,756명(42.6%), 경력은 2,365명(57.4%)인 것으로 조사되었다.

[표 3-25] 정보보호산업 채용 계획

(2020년 예상)

구분	정보보안			물리보안			합계		
	신입	경력	소계	신입	경력	소계	신입	경력	합계
인원수(명)	625	709	1,334	1,131	1,656	2,787	1,756	2,365	4,121
비중(%)	46.9	53.1	100.0	40.6	59.4	100.0	42.6	57.4	100.0

매출액 규모별로 살펴보면 100억 이상 기업에서 3,493명(84.8%), 종사자 규모별로 살펴보면 200인 이상 기업에서 3,041명(73.8%), 기업형태로 살펴보면 일반기업이 3,176명(77.1%)을 채용할 계획인 것으로 조사되었다.

[표 3-26] 정보보호 기업 특성별 채용 계획

(2020년 예상) (단위 : 명)

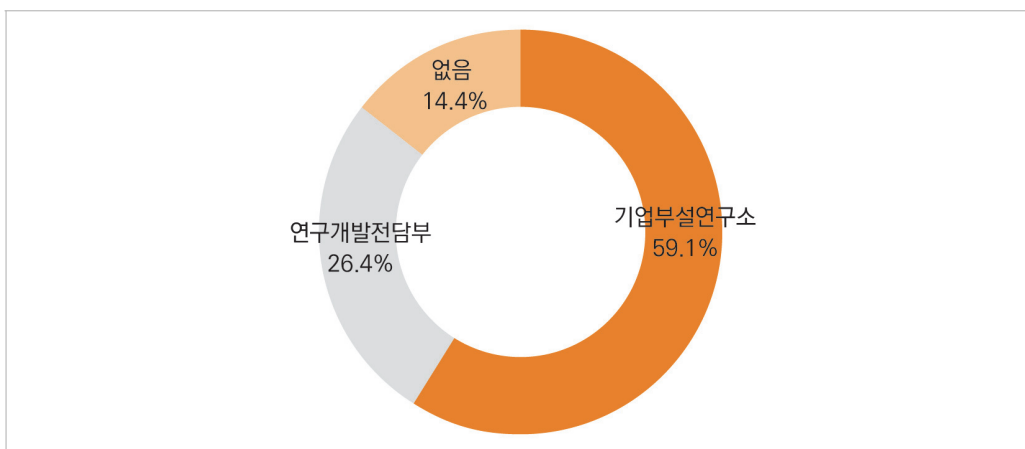
구분		계획 인원			
		정보보안	물리보안	합계	비중(%)
매출액 규모	10억 미만	42	35	77	1.9
	10억 이상-50억 미만	224	157	381	9.2
	50억 이상-100억 미만	126	44	170	4.1
	100억 이상	942	2,551	3,493	84.8
종사자 규모	20인 미만	141	63	204	5.0
	20인-100인 미만	273	181	454	11.0
	100인-200인 미만	196	226	422	10.2
	200인 이상	724	2,317	3,041	73.8
기업형태	일반기업	923	2,253	3,176	77.1
	벤처기업	411	534	945	22.9

제5절 기술개발 및 동향

정보보호 기업들의 자체기술연구소 및 연구개발 전담부서 운영 실태를 살펴보면 기업의 59.1%는 기업부설연구소를 운영하고 있으며, 연구개발 전담부서 운영이 26.4%로 조사되었다. 기업부설연구소나 연구개발 전담부서를 운영하지 않는 기업은 14.4%로 조사되었다.

[그림 3-1] 자체기술연구소 및 연구개발 전담부서 운영 현황

(단위 : %)



한편, 기술개발 시 가장 큰 애로사항으로는 정보보안과 물리보안 기업 모두 ‘기술개발 인력 확보 및 유지’(정보 40.7%, 물리 30.4%)로 조사되었으며, 다음으로 ‘자금조달’(정보 27.2%, 물리 34.1%)로 파악되었다. 다음으로 ‘기술정보 부족 및 획득 곤란’, ‘신기술의 짧은 수명주기’, ‘연구설비 기자재 부족’ 순으로 어려움을 겪는 것으로 조사되었다.

[표 3-27] 기술개발시 애로사항(중복응답)

(단위 : %)

구분	정보보안	물리보안
기술개발 인력 확보 및 유지	40.7	30.4
자금조달	27.2	34.1
기술정보 부족 및 획득 곤란	9.6	9.6
연구 설비 기자재 부족	8.0	4.4
신기술의 짧은 수명주기	8.3	15.6
기타	6.2	5.9
합계	100.0	100.0

정보보호 기업들의 지식재산권 보유 현황을 살펴보면 현재 보유중인 지식재산권이 총 7,093건, 현재 출원 중인 지식재산권이 770건인 것으로 조사되었다. 정보보안 기업의 경우 현재 보유 중인 지식재산권이 2,120건이었으며, 426건을 출원 중인 것으로 조사되었다. 물리보안 기업의 경우 4,973건을 현재 보유 중이며, 344건이 현재 출원 중인 것으로 조사되었다.

[표 3-28] 지식재산권 보유 현황

(단위 : 건)

구분	현재보유	현재 출원 중
정보보안	2,120	426
물리보안	4,973	344
합계	7,093	770

또한 정보보호 시장 활성화를 위한 정부의 정책에 대해서는 ‘자금 지원 및 세제혜택’, ‘공공부문의 시장수요 창출’, ‘기술개발 지원’, ‘법/제도 제 개정’ 등의 요구가 높은 것으로 조사되었다.

[표 3-29] 시장 확대를 위한 정부 지원 필요 사항(복수응답)

(단위 : %)

지원 요구 사항	정보보안	물리보안
전문인력 양성	18.9	7.1
기술개발 지원	34.1	28.0
기술이전의 활성화	6.8	6.2
법/제도 제 개정	6.5	11.8
공공부문의 시장수요 창출	10.8	9.5
소비촉진/투자활성화	4.3	6.6
자금지원 및 세제혜택	15.8	27.5
해외지원 사업 확대	2.2	2.4
기타	0.6	0.9
합계	100.0	100.0



제4장 정보보안산업 현황

제1절	기업 현황	39
제2절	매출 현황	44
제3절	수출 현황	57
제4절	인력 및 채용 현황	67
제5절	기술개발 및 동향	76

4장

정보보안산업 현황

제1절 기업 현황

1 지역별 현황

정보보안 관련 기업체의 소재지를 분석한 결과 473개 기업 가운데 326개 기업 (68.9%)이 서울에 소재하고 있는 것으로 조사되었다. 그 다음으로 경기 53개(11.2%), 대전 27개(5.7%), 부산 13개(2.7%) 순으로 조사되었다. 서울, 경기, 인천 수도권에 정보보안 기업의 81.2%가 집중되어 있는 것으로 나타났다.

[표 4-1] 정보보안 기업의 지역별 분포

지역	기업수(개)	비율(%)
서울	326	68.9
경기	53	11.2
대전	27	5.7
부산	13	2.7
대구	9	1.9
광주	7	1.5
전남	7	1.5
경남	6	1.3
경북	5	1.1
인천	5	1.1
제주	3	0.6
충남(세종)	3	0.6
충북	3	0.6
강원	2	0.4
울산	2	0.4
전북	2	0.4
합계	473	100.0

2 기업 형태별 현황

정보보안 관련 기업체의 형태별 현황을 살펴보면 일반기업이 309개(65.3%), 벤처기업이 164개(34.7%)인 것으로 조사되었다.

[표 4-2] 정보보안 기업 형태별 현황

구분	일반기업	벤처기업	합계
기업수(개)	309	164	473
비율(%)	65.3	34.7	100.0

3 상장 유무별 현황

정보보안 관련 기업체의 상장 유무별 현황을 살펴보면 비상장 기업이 404개(85.4%), 코스닥 기업이 57개(12.1%), 유가증권시장 기업이 5개(1.0%), 코넥스 기업이 7개(1.5%)인 것으로 조사되었다.

[표 4-3] 정보보안 기업 상장 유무별 현황

구분	비상장	코스닥	유가증권	코넥스	합계
기업수(개)	404	57	5	7	473
비율(%)	85.4	12.1	1.0	1.5	100.0

4 설립연도별 현황

정보보안 관련 기업체의 설립연도별 현황을 살펴보면 2000년 이전 설립 기업이 105개(22.2%), 2000년 이후 2005년 이전 설립 기업이 135개(28.5%), 2005년 이후 2010년 이전 설립 기업이 105개(22.2%), 2010년 이후 설립 기업이 128개(27.1%)로 조사되었다.

[표 4-4] 정보보안 기업 설립연도별 현황

구분	2000년 이전	2000년 이후- 2005년 이전	2005년 이후- 2010년 이전	2010년 이후	합계
기업수(개)	105	135	105	128	473
비율(%)	22.2	28.5	22.2	27.1	100.0

5 자본금 규모별 현황

정보보안 관련 기업체의 자본금 규모별 현황을 살펴보면 10억 미만 기업이 309개(65.3%), 10억 이상 50억 미만 기업이 114개(24.1%), 50억 이상 100억 미만 기업이 26개(5.5%), 100억 이상 기업이 24개(5.0%)인 것으로 조사되었다.

[표 4-5] 정보보안 기업 자본금 규모별 현황

구분	10억 미만	10억 이상- 50억 미만	50억 이상- 100억 미만	100억 이상	합계
기업수(개)	309	114	26	24	473
비율(%)	65.3	24.1	5.5	5.0	100.0

6 종사자 규모별 현황

정보보안 관련 기업체의 종사자 규모별 현황을 살펴보면 20인 이상 100인 미만 기업이 200개(42.2%), 20인 미만 기업이 181개(38.2%)인 것으로 조사되었다.

[표 4-6] 정보보안 기업 종사자 규모별 현황

구분	20인 미만	20인 이상- 100인 미만	100인 이상- 200인 미만	200인 이상	합계
기업수(개)	181	200	52	40	473
비율(%)	38.2	42.2	11.1	8.5	100.0

7 취급 품목별 현황

정보보안 관련 기업체의 취급하는 품목을 중분류로 구분하여 이에 포함된 제품 중 어느 하나라도 취급하면 판매에 기여하는 것으로 보고 중복으로 계수하여 취급 품목별로 정리한 결과는 [표 4-7]와 [그림 4-1]과 같다.

정보보안 시스템 개발 및 공급을 72.5%의 기업이 취급하며, 정보보안 관련 서비스를 취급하는 회사는 전체의 27.5%인 것으로 조사되었다.

제품별 취급 기업 수를 살펴보면 네트워크 보안 시스템 개발 21.5%, 시스템보안 솔루션 개발 18.7%, 정보유출방지 시스템 개발 14.2%, 보안관리 시스템 개발 13.1%, 암호/인증 시스템 개발 5.0%인 것으로 조사되었다.

정보보안 관련 서비스의 경우는 보안시스템 유지관리/보안성 지속 서비스 14.3%, 보안컨설팅 서비스 9.1%, 보안관계 서비스 2.8%, 보안교육 및 훈련 서비스 0.8%, 공인/사설 인증서 0.5%인 것으로 조사되었다.

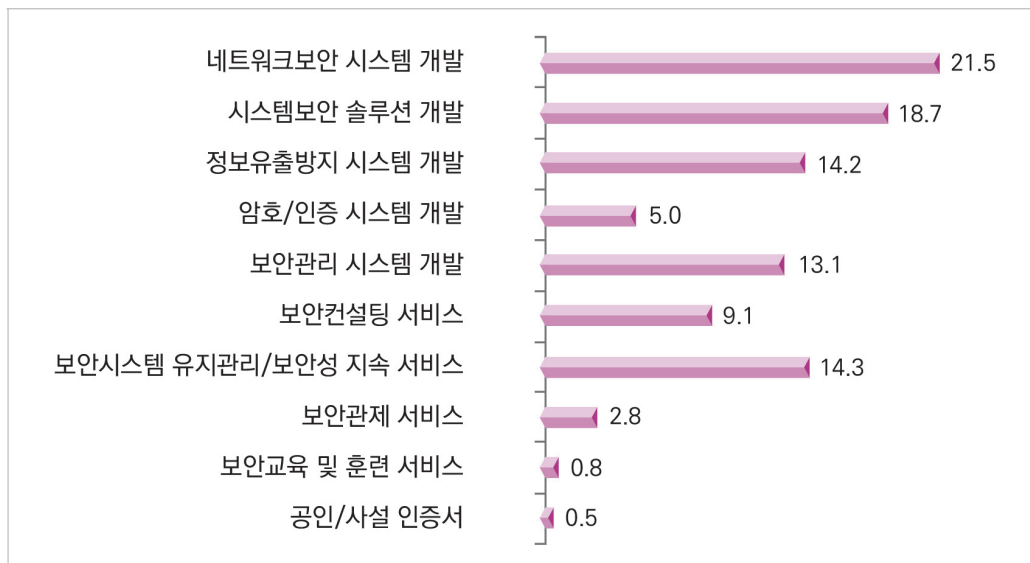
[표 4-7] 정보보안 기업의 중분류 품목별 취급 기업 현황

(단위 : 개, %)

구분		기업 수	비율(%)
정보보안 시스템 개발 및 공급	네트워크보안 시스템 개발	168	21.5
	시스템보안 솔루션 개발	146	18.7
	정보유출방지 시스템 개발	111	14.2
	암호/인증 시스템 개발	39	5.0
	보안관리 시스템 개발	102	13.1
	소계	566	72.5
정보보안 관련 서비스	보안컨설팅 서비스	71	9.1
	보안시스템 유지관리/ 보안성 지속 서비스	112	14.3
	보안관제 서비스	22	2.8
	보안교육 및 훈련 서비스	6	0.8
	공인/사설 인증서	4	0.5
	소계	215	27.5
합계		781	100.0

[그림 4-1] 정보보안기업의 중분류 품목별 취급 기업 현황

(단위 : %)



제2절 매출 현황

1 전체 매출 현황

가. 대분류 현황

정보보안산업은 2019년 3,277,687백만원의 매출을 기록하여 2018년 3,082,926백만원 대비 6.32% 증가한 것으로 조사되었다. 이 중에서 정보보안 시스템 개발 및 공급은 2019년 2,240,572백만원으로 2018년 2,093,723백만원 대비 7.01% 증가하였으며, 정보보안 관련 서비스는 2019년 1,037,115백만원으로 2018년 989,203백만원 대비 4.84% 증가한 것으로 조사되었다.

[표 4-8] 정보보안산업 대분류 매출 현황

(단위: 백만원, %)

구분	2018년	2019(E)	증감율(%)
정보보안 시스템 개발 및 공급	2,093,723	2,240,572	7.01
정보보안 관련 서비스	989,203	1,037,115	4.84
합계	3,082,926	3,277,687	6.32

나. 중분류 현황

정보보안산업의 중분류별 매출을 살펴보면, 정보보안 시스템 개발 및 공급은 네트워크 보안 시스템 개발, 정보유출방지 시스템 개발, 시스템보안 솔루션 개발 분야의 매출 비중이 높으며, 정보보안 관련 서비스는 보안관계 서비스, 보안컨설팅 서비스, 유지관리/보안성 지속 서비스 분야의 매출 비중이 높은 것으로 조사되었다. 정보보안 시스템 개발 및 공급 부문에서는 네트워크보안 시스템 개발의 수요가 증가한 것으로 분석되며, 정보보안 관련 서비스 부문에서는 보안 공격의 지능화, 고도화, 복잡/다양화에 대응하기 위한 보안관계, 보안컨설팅, 유지관리/보안성 지속 서비스가 증가하는 것으로 분석되었다.

[표 4-9] 정보보안산업 중분류 매출 현황

(단위 : 백만원, %)

구분		2018년	2019년	증감율(%)
정보보안 시스템 개발 및 공급	네트워크보안 시스템 개발	729,393	771,656	5.8
	시스템보안 솔루션 개발	488,402	523,115	7.1
	정보유출방지 시스템 개발	426,128	456,251	7.1
	암호/인증 시스템 개발	151,879	161,760	6.5
	보안관리 시스템 개발	297,920	327,790	10.0
	소계	2,093,723	2,240,572	7.0
정보보안 관련 서비스	보안컨설팅 서비스	302,099	321,478	6.4
	보안시스템유지관리/ 보안성 지속 서비스	351,942	359,645	2.2
	보안관제 서비스	273,927	286,880	4.7
	보안교육 및 훈련 서비스	1,740	2,990	71.8
	공인/사설 인증서	59,496	66,122	11.1
	소계	989,203	1,037,115	4.8
합계		3,082,926	3,277,687	6.3

다. 업종별 매출 현황

정보보안 시스템 개발 및 공급 분야의 업종별 매출비중은 일반기업 업종부문이 45.9%의 가장 높은 매출 비중을 보였고, 다음으로 공공 업종 35.3%, 금융기관 업종 18.8% 순으로 나타났다. 정보보안 관련 서비스의 업종별 매출비중에서는 일반업종 부문이 가장 많은 52.9%의 매출 비중을 보였으며, 공공기업 업종 28.2%, 금융기관 업종 18.9%로 각각 조사되었다.

[표 4-10] 정보보안산업 업종별(수요처별) 매출 현황

(단위 : %)

구분	업종(수요처)			
	공공	금융	일반기업	합계
정보보안 시스템 개발 및 공급	35.3	18.8	45.9	100.0
정보보안 관련 서비스	28.2	18.9	52.9	100.0

2 특성별 매출 현황

2019년 정보보안 총 매출액은 3,277,687백만원이며, 기업 특성별로 정보보안 총매출액과 평균 매출액은 [표 4-11]와 같다.

[표 4-11] 정보보안산업 특성별 매출 현황(2019년)

(단위: 백만원)

분류		매출액	평균	분류		매출액	평균
지역	서울	2,449,442	7,514	설 립 연 도	2000년 이전	1,369,682	13,045
					2000년 이후- 2005년 이전	1,098,279	8,135
	서울 외	828,245	5,634		2005년 이후- 2010년 이전	319,380	3,042
					2010년 이후	490,347	3,831
상장 유무	비상장	1,866,790	4,621	종 사 자	20인 미만	299,426	1,654
	코스닥	1,152,991	20,228		20인-100인 미만	952,197	4,761
	유가증권	193,054	38,611		100인-200인 미만	563,804	10,842
	코넥스	64,852	9,265		200인 이상	1,462,259	36,556
기업 형태	일반기업	2,208,879	7,148	자 본 금	10억 미만	734,458	2,377
					10억-50억 미만	874,190	7,668
	벤처기업	1,068,809	6,517		50억-100억 미만	1,127,760	43,375
					100억 이상	541,279	22,553

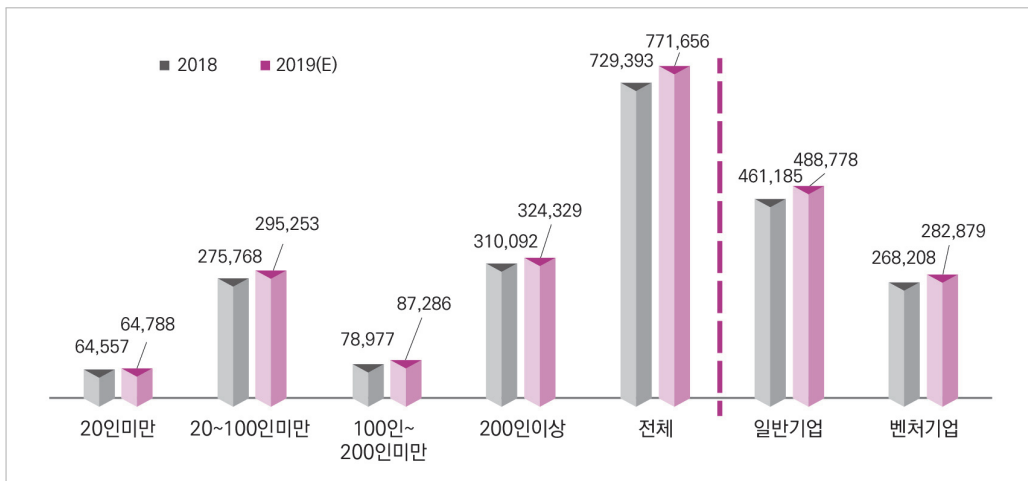
3 제품별 매출 현황

가. 네트워크 보안 시스템 개발

2018년 매출은 729,393백만원이며, 2019년 매출은 771,656백만원으로 5.79%의 증가가 예상된다. 20인 이상 100인 미만 기업의 매출액은 295,253백만원이며, 200인 이상 매출액은 324,329백만원으로 종사자가 200인 이상인 기업에서 주로 판매되는 것으로 나타났다. 일반기업의 매출액은 488,778백만원이며, 벤처기업의 매출액은 282,879백만원으로 일반기업의 매출액이 벤처기업의 매출액보다 높은 것으로 나타났다.

[그림 4-2] 네트워크 보안 시스템 개발 매출 현황

(단위 : 백만원)

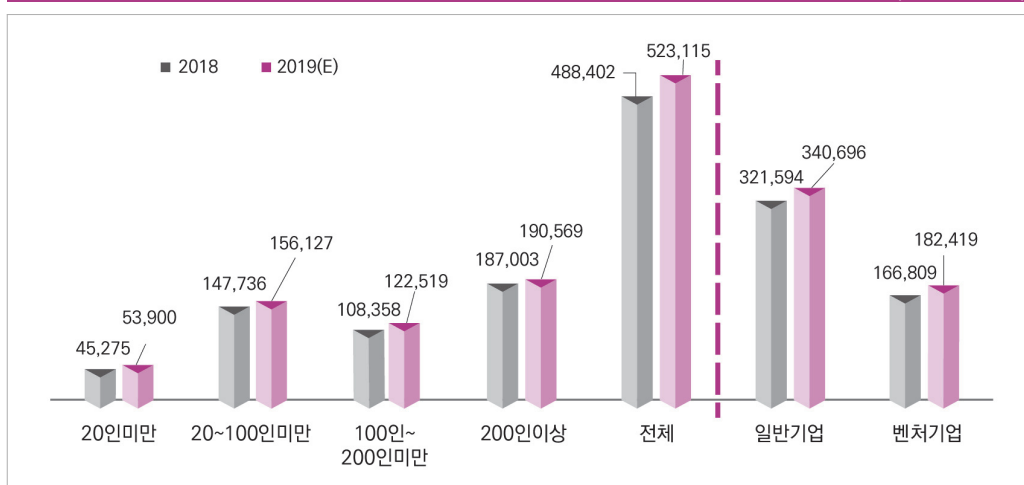


나. 시스템 보안 솔루션 개발

2018년 매출은 488,402백만원이며, 2019년 매출은 523,115백만원으로 7.08%의 증가가 예상된다. 20인 이상 100인 미만 기업의 매출액은 156,127백만원이며, 200인 이상 매출액은 190,569백만원으로 종사자가 200인 이상인 기업에서 주로 판매되는 것으로 나타났다. 일반기업의 매출액은 340,696백만원이며, 벤처기업의 매출액은 182,419만원으로 일반기업의 매출액이 벤처기업의 매출액보다 높은 것으로 나타났다.

[그림 4-3] 시스템 보안 솔루션 개발 매출 현황

(단위 : 백만원)

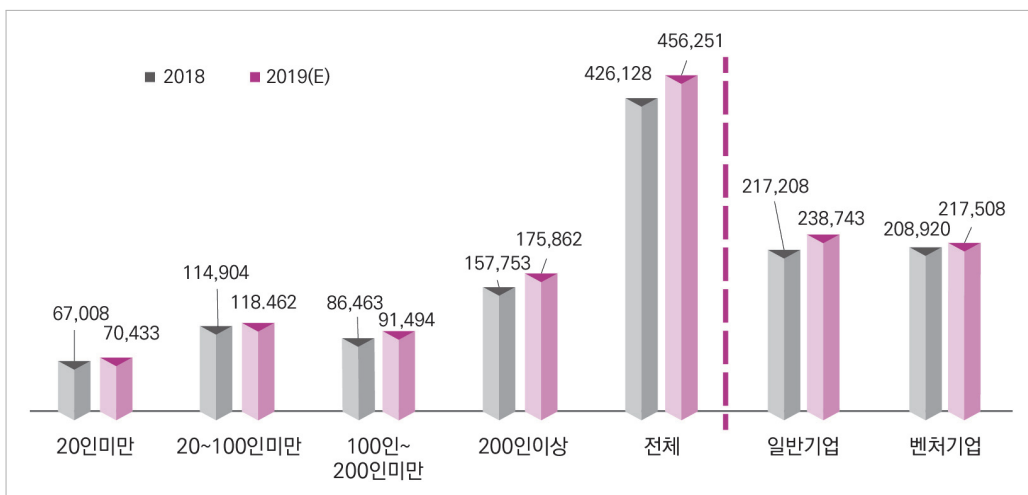


다. 정보유출방지 시스템 개발

2018년 매출은 426,128백만원이며, 2019년 매출은 456,251백만원으로 7.05%의 증가가 예상된다. 20인 이상 100인 미만 기업의 매출액은 118,462백만원이며, 200인 이상 매출액은 175,862백만원으로 종사자가 200인 이상인 기업에서 주로 판매되는 것으로 나타났다. 일반기업의 매출액은 238,743백만원이며, 벤처기업의 매출액은 217,508백만원으로 일반기업의 매출액이 벤처기업의 매출액보다 다소 높은 것으로 나타났다.

[그림 4-4] 정보유출방지 시스템 개발 매출 현황

(단위 : 백만원)

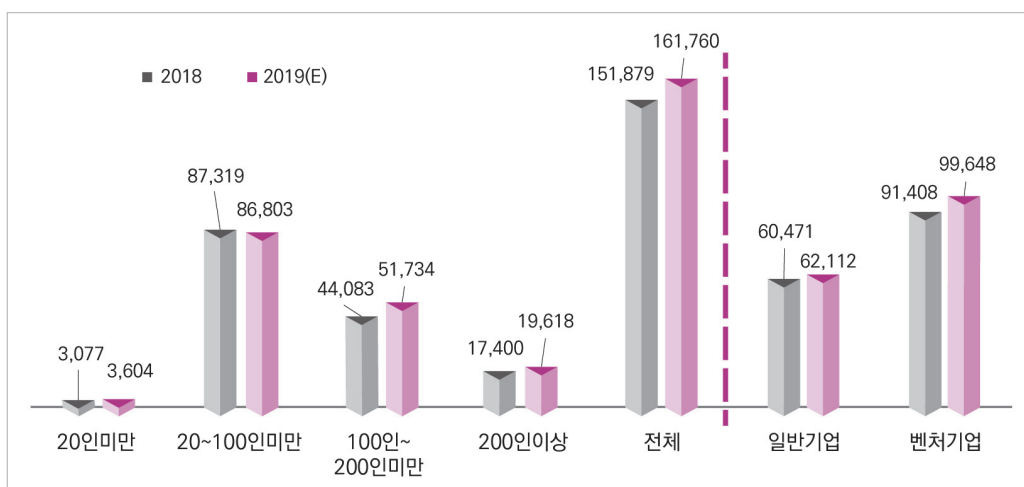


라. 암호/인증 시스템 개발

2018년 매출은 151,879백만원이며, 2019년 매출은 161,760백만원으로 6.48%의 증가가 예상된다. 20인 이상 100인 미만 기업의 매출은 86,803백만원이며, 100인 이상 200인 미만 기업의 매출액은 51,734백만원으로 종사자가 20인 이상 100인 미만인 기업에서 주로 판매되는 것으로 나타났다. 일반기업의 매출액은 62,112백만원이며, 벤처기업의 매출액은 99,648백만원으로 일반기업의 매출액이 벤처기업의 매출액보다 낮은 것으로 나타났다.

[그림 4-5] 암호/인증 시스템 개발 매출 현황

(단위 : 백만원)

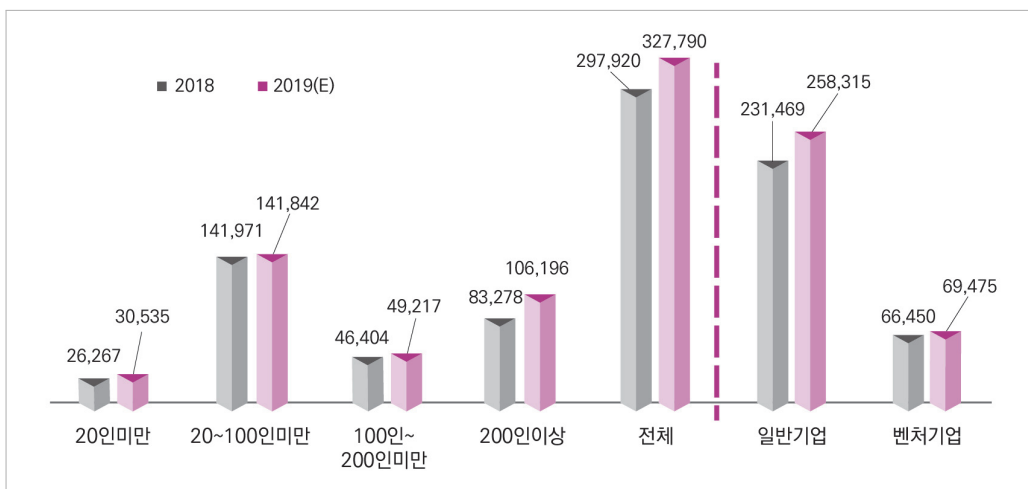


마. 보안관리 시스템 개발

2018년 매출은 297,920백만원이며, 2019년 매출은 327,790백만원으로 10.02%의 증가가 예상된다. 20인 이상 100인 미만 기업의 매출은 141,842백만원이며, 200인 이상 매출액은 106,196백만원으로 종사자가 20인 이상 100인 미만인 기업에서 주로 판매되는 것으로 나타났다. 일반기업의 매출액은 258,315백만원이며, 벤처기업의 매출액은 69,475백만원으로 일반기업의 매출액이 벤처기업의 매출액보다 높은 것으로 나타났다.

[그림 4-6] 보안관리 시스템 매출 현황

(단위 : 백만원)



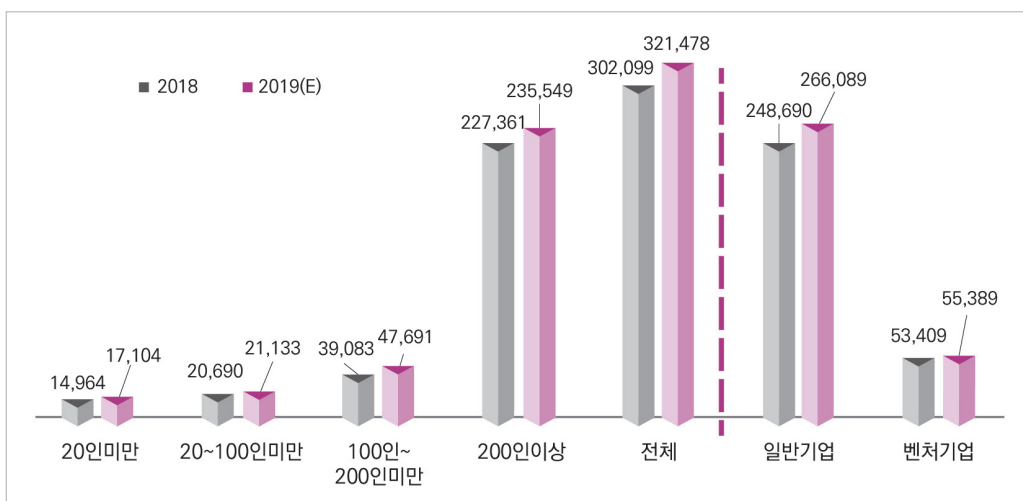
4 서비스별 매출 현황

가. 보안컨설팅 서비스

2018년 매출은 302,099백만원이며, 2019년 매출은 321,478백만원으로 6.41%의 증가가 예상된다. 100인 이상 200인 미만 기업의 매출은 47,691백만원이며, 200인 이상 매출액은 235,549백만원으로 종사자가 200인 이상인 기업에서 주로 판매되는 것으로 나타났다. 일반기업의 매출액은 266,089백만원이며, 벤처기업의 매출액은 55,389백만원으로 일반기업의 매출액이 벤처기업의 매출액보다 높은 것으로 나타났다.

[그림 4-7] 보안컨설팅 서비스 매출 현황

(단위 : 백만원)

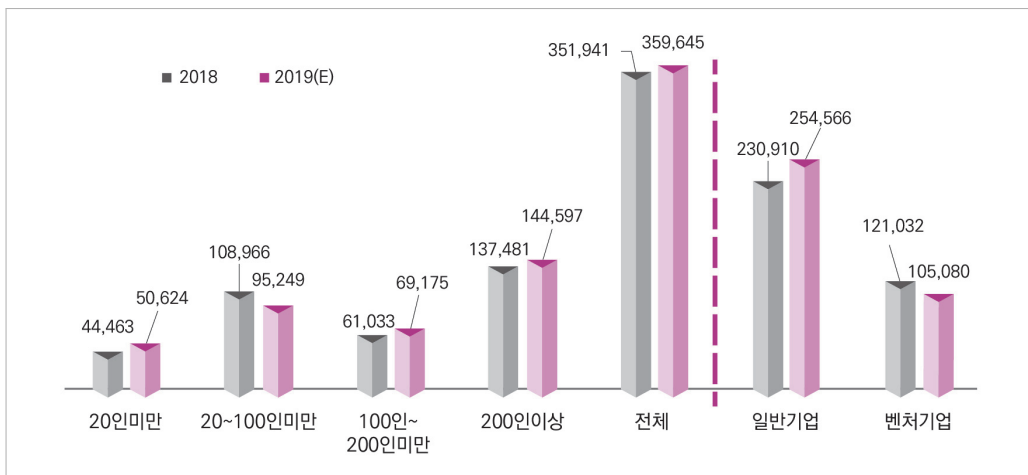


나. 보안시스템 유지관리/보안성 지속 서비스

2018년 매출은 351,942백만원이며, 2019년 매출은 359,645백만원으로 2.18%의 증가가 예상된다. 20인 이상 100인 미만 기업의 매출은 95,249백만원이며, 200인 이상 매출액 144,597백만원으로 종사자가 200인 이상인 기업에서 주로 판매되는 것으로 나타났다. 일반기업의 매출액은 254,566백만원이며, 벤처기업의 매출액은 105,080백만원으로 일반기업의 매출액이 벤처기업의 매출액보다 높은 것으로 나타났다.

[그림 4-8] 보안시스템 유지관리/보안성 지속 서비스 매출 현황

(단위 : 백만원)

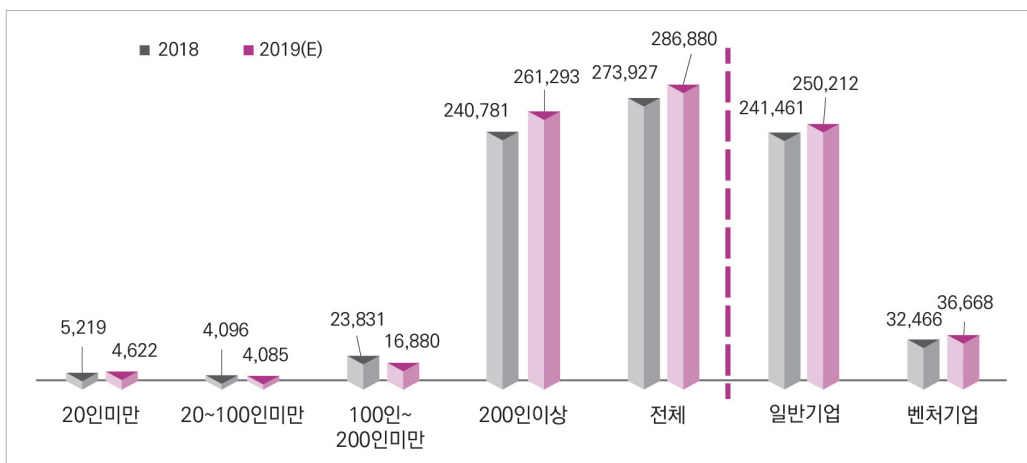


다. 보안관제 서비스

2018년 매출은 273,927백만원이며, 2019년 매출은 286,880백만원으로 4.72%의 증가가 예상된다. 100인 이상 200인 미만 기업의 매출은 16,880백만원이며, 200인 이상 매출액은 261,293백만원으로 종사자가 200인 이상인 기업에서 주로 판매되는 것으로 나타났다. 일반기업의 매출액은 250,212백만원이며, 벤처기업의 매출액은 36,668백만원으로 일반기업의 매출액이 벤처기업의 매출액보다 높은 것으로 나타났다.

[그림 4-9] 보안관제 서비스 매출 현황

(단위 : 백만원)

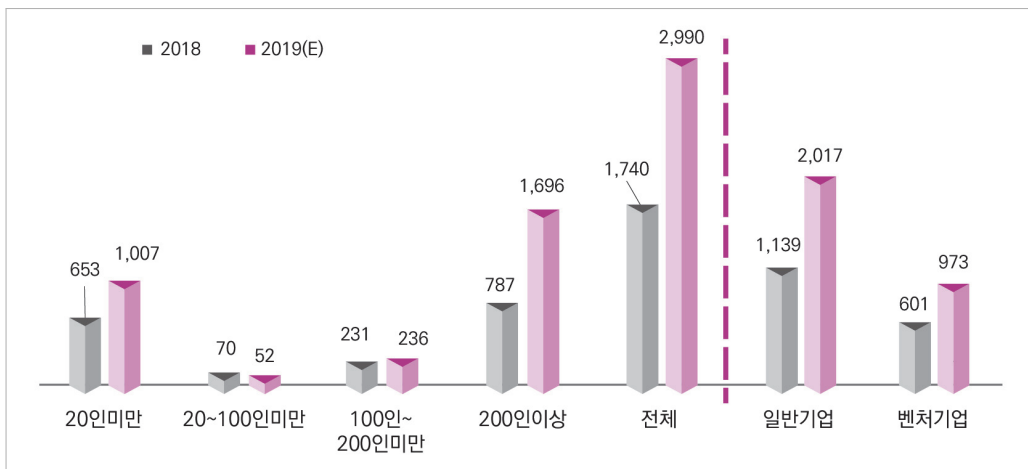


라. 보안교육 및 훈련 서비스

2018년 매출은 1,740백만원이며, 2019년 매출은 2,990백만원으로 71.83%의 증가가 예상된다. 20인 미만 기업의 매출은 1,007백만원이며, 200인 이상 매출액은 1,696백만원으로 종사자가 200인 이상인 기업에서 주로 판매되는 것으로 나타났다. 일반기업의 매출액은 2,017백만원이며, 벤처기업의 매출액은 973백만원으로 일반기업의 매출액이 벤처기업의 매출액보다 높은 것으로 나타났다.

[그림 4-10] 보안교육 및 훈련 서비스 매출 현황

(단위 : 백만원)

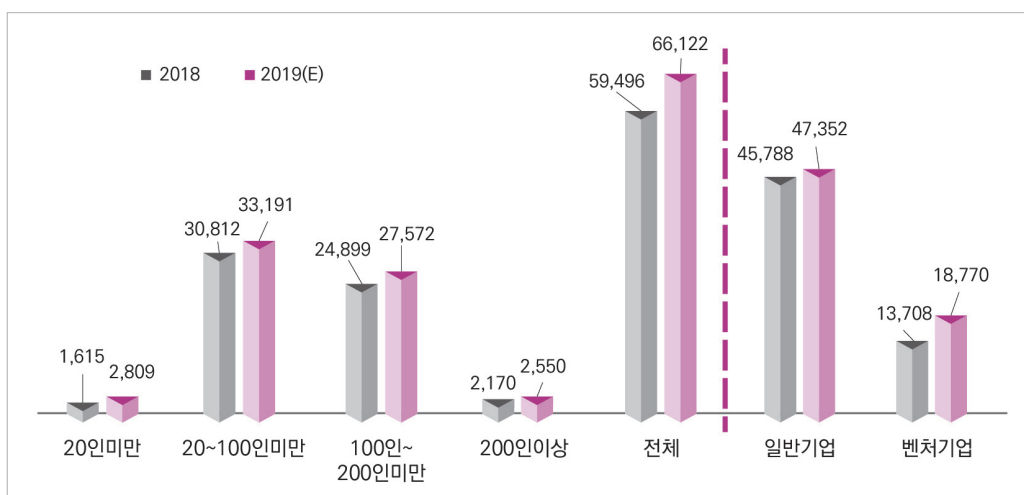


마. 공인/사설 인증서

2018년 매출은 59,496백만원이며, 2019년 매출은 66,122백만원으로 11.14%의 증가가 예상된다. 공인/사설 인증서는 종사자가 20인 이상 100인 미만 기업의 매출이 33,191백만원, 100인 이상 200인 미만 기업의 매출이 27,572백만원으로, 종사자가 20인 이상 100인 미만인 기업에서 주로 판매되는 것으로 나타났다. 또한 일반기업의 매출액은 47,352백만원이며, 벤처기업의 매출액은 18,770백만원으로 일반기업의 매출액이 벤처기업의 매출액보다 높은 것으로 나타났다.

[그림 4-11] 공인/사설 인증서 매출 현황

(단위 : 백만원)



제3절 수출 현황

정보보안산업 수출액은 2018년 82,363백만원이었으며, 2019년도 수출액은 108,528백만원으로 31.8% 증가할 것으로 조사되었다. 2019년 수출비중을 살펴보면 정보보안 시스템 개발 및 공급의 수출이 전체 수출의 65.4%로 정보보안 관련 서비스(34.6%)의 수출은 상대적으로 미약한 수준이다.

[표 4-12] 정보보안 대분류별 수출 현황

(단위 : 백만원, %)

구분	2018년	2019년(E)	증감율(%)	비중(%)
정보보안 시스템 개발 및 공급	62,943	70,980	12.8	65.4
정보보안 관련 서비스	19,420	37,549	93.4	34.6
합계	82,363	108,528	31.8	100.0

분야별로 살펴보면 정보보안 시스템 개발 및 공급군에서는 네트워크보안 시스템 개발 제품이 수출시장에서 차지하는 규모가 2019년 33,574백만원으로 가장 크며, 다음으로 시스템보안 솔루션 개발 제품이 14,813백만원으로 나타났다. 수출 증가율이 두드러질 것으로 예상되는 제품은 정보유출방지 시스템 개발 제품(24.2%), 네트워크보안 시스템 개발(21.5%) 등이 상대적으로 큰 증가율을 보이고 있다.

정보보안 관련 서비스 중 2019년 수출액은 보안컨설팅 서비스가 22,017백만원으로 크게 나타났으며, 271.01%의 증가율을 보이는 것으로 나타났다.

[표 4-13] 정보보안 제품 및 서비스 수출 현황

(단위 : 백만원, %)

구분		2018년	2019년(E)	증감율(%)
정보보안 시스템 개발 및 공급	네트워크보안 시스템 개발	27,642	33,574	21.5
	시스템보안 솔루션 개발	15,319	14,814	-3.3
	정보유출방지 시스템 개발	9,926	12,324	24.2
	암호/인증 시스템 개발	3,032	3,108	2.5
	보안관리 시스템 개발	7,024	7,159	1.9
정보보안 관련 서비스	보안컨설팅 서비스	5,934	22,017	271.0
	보안시스템 유지관리/ 보안성 지속 서비스	9,594	10,054	4.8
	보안관제 서비스	3,892	5,478	40.8
합계		82,363	108,528	31.8

수출 대상 국가의 비중을 살펴보면 일본으로의 수출 비중이 가장 높게 나타났다. 정보보안 시스템 개발 및 공급의 경우 일본 수출 비중이 45.6%였으며, 정보보안 관련 서비스의 경우 일본 수출 비중이 61.1%인 것으로 조사되었다. 또한, 정보보안 시스템 개발 및 공급의 경우 중국 14.8%, 미국과 유럽의 경우 각각 6.9%, 1.2%의 수출 비중을 보이고 있고, 기타 지역으로의 수출은 31.5%로 나타났다. 기타 지역으로는 동남아시아와 남미의 응답이 많이 나타났다.

[표 4-14] 정보보안 국가별 수출 현황(2018)

(단위 : %)

구분	수출 국가					
	일본	중국	미국	유럽	기타	합계
정보보안 시스템 개발 및 공급	45.6	14.8	6.9	1.2	31.5	100.0
정보보안 관련 서비스	61.1	30.6	1.1	0.3	6.8	100.0

1 정보보안 시스템 개발 및 공급 수출 현황

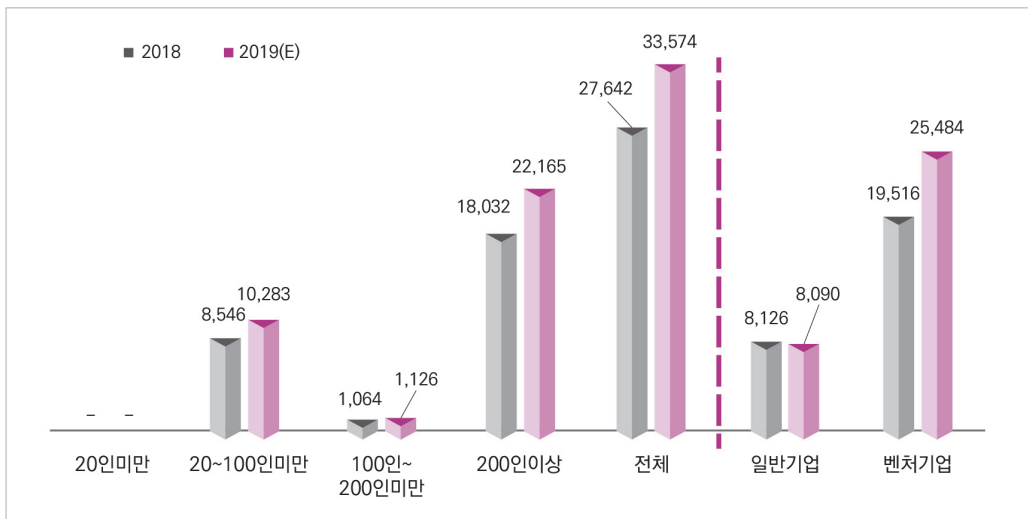
가. 네트워크보안 시스템 개발

네트워크보안 시스템 개발은 가상사설망(VPN), 네트워크 접근제어(NAC), 네트워크(시스템) 방화벽, 기타, 웹방화벽, 차세대 방화벽(NGFW), 침입방지시스템(IPS), 통합보안시스템(UTM), DDoS 차단시스템, 망분리(가상화) 등의 제품으로 이들 제품의 2019년 수출 예상액은 33,574백만원으로 2018년 27,642백만원 보다 21.5% 증가한 것으로 조사되었다.

2019년 네트워크 보안 제품은 200인 이상 기업의 수출은 22,165백만원이며, 20인 이상 100인 미만의 기업의 수출이 10,283백만원으로 나타났다. 또한 벤처기업의 수출액이 일반기업의 수출액보다 높은 것으로 나타났다.

[그림 4-12] 네트워크보안 시스템 개발 수출 현황

(단위 : 백만원)



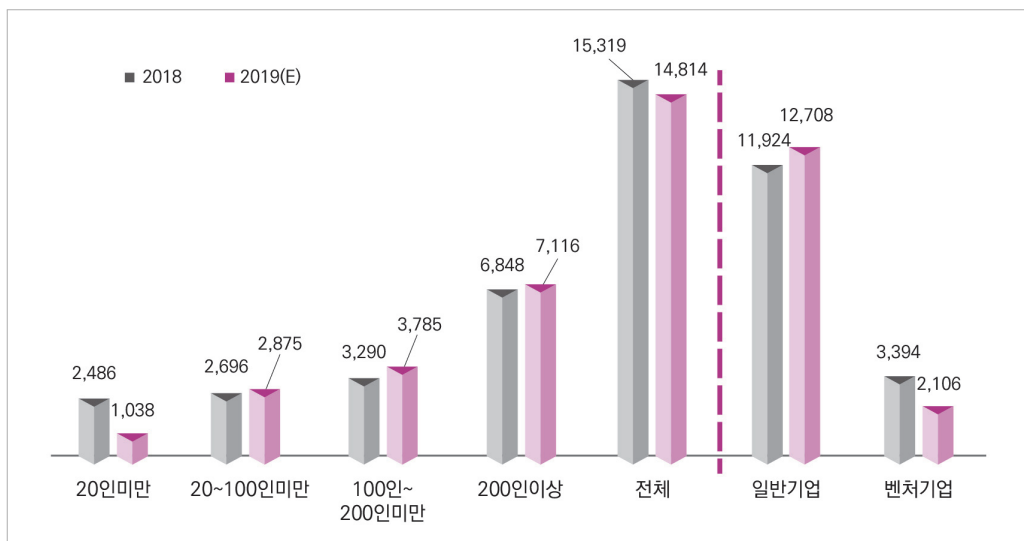
나. 시스템보안 솔루션 개발

시스템보안 솔루션 개발은 APT대응, 멀웨어 대응, 모바일 보안, 보안운영체제(Secure OS), 스팸차단 솔루션, 시스템 접근 통제(PC방화벽 포함), 엔드포인트 탐지 및 대응(EDR)이 해당되는데 이들 제품의 2019년 수출액 예상액은 14,814백만원으로 2018년 15,319백만원 보다 3.3% 감소한 것으로 조사되었다.

2019년 시스템보안 솔루션 개발은 200인 이상 기업의 수출이 7,116백만원이며, 100인 이상 200인 미만 기업의 수출은 3,785백만원으로 나타났다. 또한 일반기업의 수출액이 벤처기업의 수출액보다 많은 것으로 나타났다.

[그림 4-13] 시스템보안 솔루션 개발 수출 현황

(단위 : 백만원)



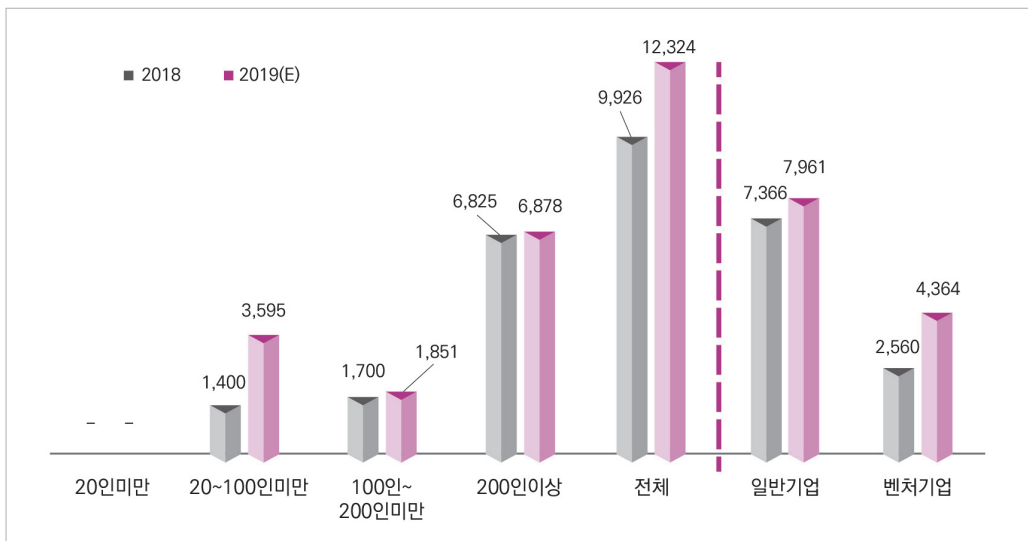
다. 정보유출방지 시스템 개발

정보유출방지 시스템 개발은 DB보안(접근통제), DB암호, 네트워크 DLP, 단말 DLP(개인정보 솔루션 포함), 디지털저작권관리(DRM), 보안USB 등이 해당되는데 2019년 12,324백만원을 수출하여, 2018년 9,926백만원 보다 24.2% 상승한 것으로 조사되었다.

2019년 수출은 종사자 수 200인 이상 기업의 수출은 6,878백만원, 20인 이상 100인 미만 기업의 수출이 3,595백만원으로 나타났으며, 일반기업이 벤처기업보다 수출액이 높게 나타났다.

[그림 4-14] 정보유출방지 시스템 개발 수출 현황

(단위 : 백만원)



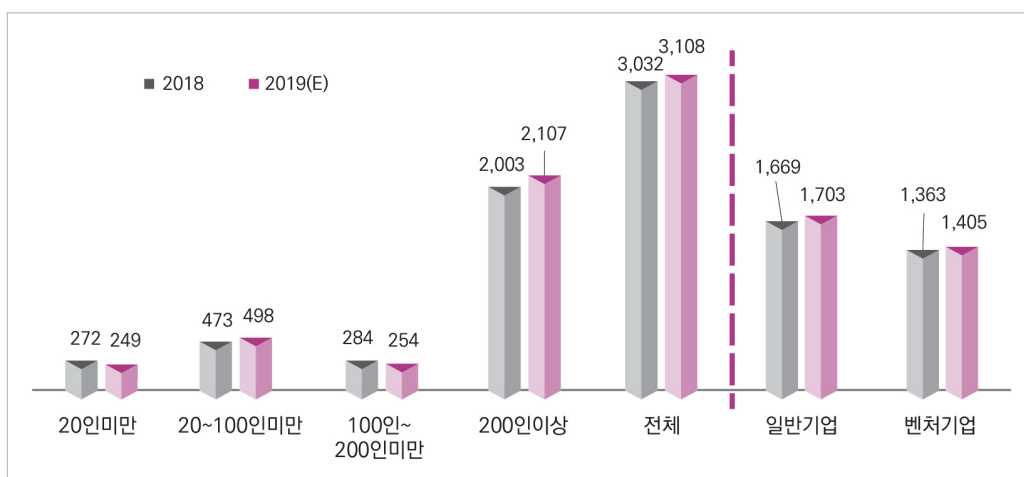
라. 암호/인증 시스템 개발

암호/인증 시스템 개발은 공개키기반구조(PKI), 기타, 일회용비밀번호(OTP), 통합 접근관리(EAM)/싱글사인온(SSO)이 해당되는데 2019년 3,108백만원을 수출하여, 2018년 3,032백만원 보다 2.5% 상승한 것으로 조사되었다.

2019년 수출은 종사자 수 200인 이상 기업의 수출이 2,107백만원, 20인 이상 100인 미만 기업의 수출은 498백만원으로 나타났으며, 일반기업의 수출액이 벤처기업의 수출액보다 높은 것으로 나타났다.

[그림 4-15] 암호/인증 시스템 개발 수출 현황

(단위 : 백만원)



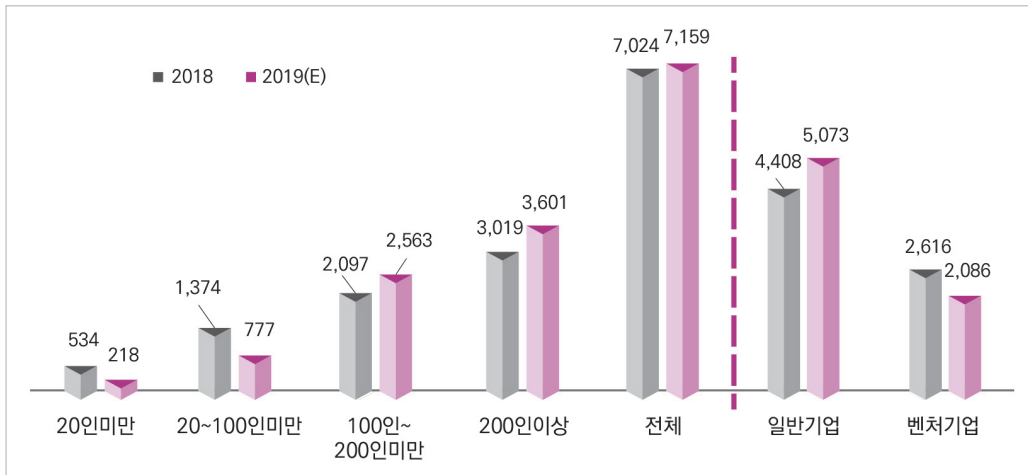
마. 보안관리 시스템 개발

보안관리 시스템 개발은 디지털 포렌식 시스템, 위협관리시스템(TMS), 패치관리 시스템(PMS), 백업/복구 관리 시스템, 로그 관리/분석 시스템, 취약점 분석 시스템, 통합 보안관제시스템(SIEM) 등이 해당되는데 이들 제품의 2019년 수출액은 7,159백만원으로 2018년 7,024백만원보다 1.9% 증가한 것으로 조사되었다.

2019년 보안관리 시스템 개발 제품의 수출은 종사자 수 100인 이상 200인 미만 기업에서 2,563백만원, 200인 이상 기업에서 3,601백만원으로 나타났다. 또한 일반기업의 수출액이 벤처기업의 수출액보다 높은 것으로 나타났다.

[그림 4-16] 보안관리 시스템 개발 수출 현황

(단위 : 백만원)



2 정보보안 관련 서비스 수출현황

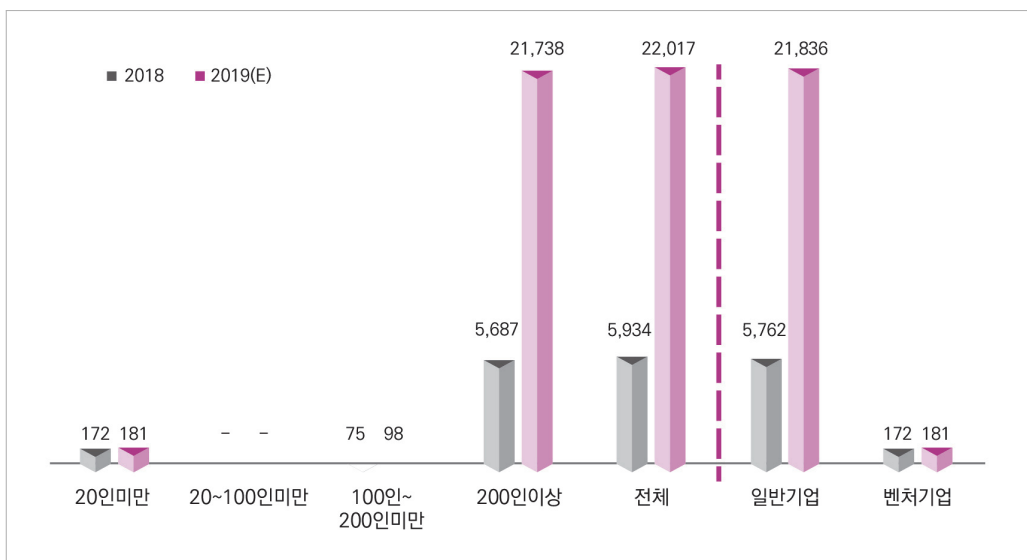
가. 보안컨설팅 서비스

보안컨설팅 서비스의 수출액은 2019년 22,017백만원으로 2018년 5,934백만원에 비해 271% 상승하는 것으로 조사되었다.

보안컨설팅 서비스는 종사자 수 200인 이상 기업의 수출이 21,738백만원이며, 20인 미만 기업의 수출은 181백만원으로 나타났다. 또한 일반기업의 수출액이 대부분을 차지하는 것으로 나타났다.

[그림 4-17] 보안컨설팅 서비스 수출 현황

(단위 : 백만원)



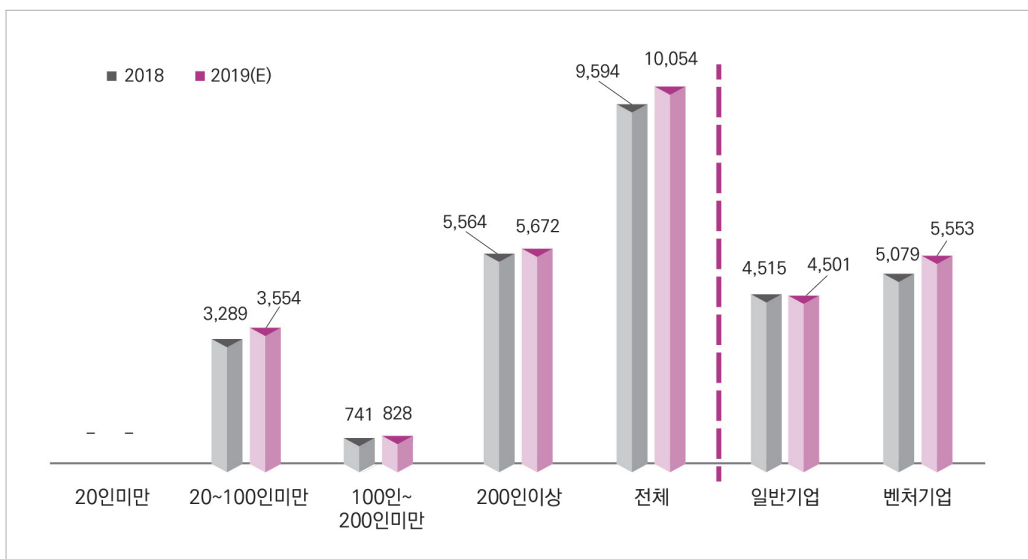
나. 보안시스템 유지관리/보안성 지속 서비스

보안시스템 유지관리/보안성 지속 서비스의 수출액은 2019년 10,054백만원으로 2018년 9,594백만원에 비해 4.8% 증가한 것으로 조사되었다.

종사자 수 200인 이상 기업의 수출이 5,672백만원이며, 20인 이상 100인 미만 기업의 수출은 3,554백만원으로 나타났다. 또 벤처기업의 수출액이 일반기업의 수출액보다 다소 높은 것으로 나타났다.

[그림 4-18] 보안시스템 유지관리/보안성 지속 서비스 수출 현황

(단위 : 백만원)



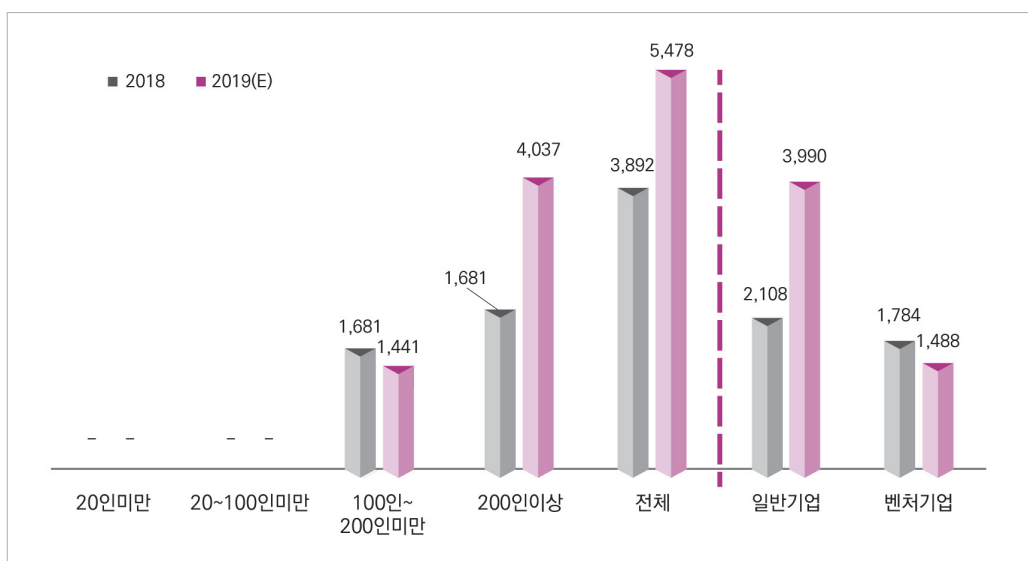
다. 보안관제 서비스

보안관제 서비스의 수출액은 2019년 5,478백만원으로 2018년 3,892백만원에 비해 40.8% 상승하는 것으로 조사되었다.

보안관제 서비스는 200인 이상 기업의 수출이 4,037백만원이며, 100인 이상 200인 미만 기업의 수출은 1,441백만원으로 나타났다. 또한 일반기업의 수출액이 벤처기업의 수출액보다 큰 것으로 나타났다.

[그림 4-19] 보안관제 서비스 수출 현황

(단위 : 백만원)



제4절 인력 및 채용 현황

1 인력 현황

각 기업의 구분별 정보보안 담당 인력은 총 13,378명으로 조사되었다. 설립연도로 살펴보면 2005년 이후 - 2010년 이전 설립된 기업, 벤처기업에서 전체 인원 중 정보보안 인력의 비중이 높음을 알 수 있다. 또한 종사자수 200인 이상, 자본금 50억 이상 100억 미만 기업의 정보보안 인력 평균이 높게 나타났다.

[표 4-15] 정보보안산업 구분별 인력 현황

(2018년 12월 기준)

구분		기업수 (개)	정보보안 담당인력(명)		전체 인력(명)		비중(%)
		합계	합계	평균	합계	평균	
전체		473	13,378	28	28,041	59	47.7
지역	서울	326	9,395	29	20,732	64	45.3
	서울 외	147	3,983	27	7,309	50	54.5
상장 유무	비상장	404	6,937	17	16,697	41	41.5
	코스닥	57	6,139	108	8,726	153	70.4
	유가증권	5	118	24	2,268	454	5.2
	코넥스	7	184	26	350	50	52.6
기업 형태	일반기업	309	8,988	29	21,035	68	42.7
	벤처기업	164	4,390	27	7,006	43	62.7
설립 연도	2000년 이전	105	6,508	62	18,027	172	36.1
	2000년 이후- 2005년 이전	135	3,332	25	5,034	37	66.2
	2005년 이후- 2010년 이전	105	1,435	14	1,884	18	76.2
	2010년 이후	128	2,103	16	3,096	24	67.9
종사자 수	20인 미만	181	655	4	803	4	81.6
	20인-100인 미만	200	3,039	15	4,565	23	66.6
	100인-200인 미만	52	2,694	52	3,326	64	81.0
	200인 이상	40	6,990	175	19,347	484	36.1
자본금	10억 미만	309	2,804	9	4,038	13	69.4
	10억-50억 미만	114	4,093	36	7,883	69	51.9
	50억-100억 미만	26	5,417	208	7,795	300	69.5
	100억 이상	24	1,064	44	8,325	347	12.8

2 특성별 현황

정보보안 관련 인력은 총 13,378명으로 이 중에서 15년 이상이 893명(6.7%), 11년 이상 15년 미만이 1,825명(13.6%), 7년 이상 11년 미만이 2,915명(21.8%), 4년 이상 7년 미만이 3,908명(29.2%), 4년 미만이 3,837명(28.7%)인 것으로 조사되었다. 4년 이상 7년 미만 > 4년 미만 > 7년 이상 11년 미만 > 11년 이상 15년 > 15년 이상 순으로 인력이 많은 것으로 나타났다.

[표 4-16] 정보보안산업 인력 현황

(2018년 12월 현재)

구분	4년 미만	4년 이상 7년 미만	7년 이상 11년 미만	11년 이상 15년 미만	15년 이상	합계
정보보안(명)	3,837	3,908	2,915	1,825	893	13,378
비중(%)	28.7	29.2	21.8	13.6	6.7	100.0

가. 직종별 현황

특성별 및 직종별로 인력 현황을 살펴보면, 15년 이상은 총 893명이었으며 이 중 정보보안 연구 및 개발직이 279명으로 가장 많았고, 다음으로 정보시스템 관리직이 259명, 정보보안 영업직이 242명 순으로 조사되었다.

11년 이상 15년 미만의 경우, 정보보안 관리직이 748명으로 가장 많았고, 정보보안 영업직 519명, 다음으로 정보보안 연구 및 개발직이 451명 순으로 조사되었다.

7년 이상 11년 미만의 경우, 정보보안 관리직이 1,628명으로 가장 많았고, 정보보안 연구 및 개발직이 793명, 정보보안 영업직이 423명 순으로 나타났다.

4년 이상 7년 미만의 경우, 정보보안 관리직이 2,270명으로 가장 많았고, 정보보안 연구 및 개발직 1,197명, 정보보안 영업직이 382명 순으로 높게 나타났다.

4년 미만의 경우, 정보보안 연구 및 개발직이 1,877명으로 가장 많았고, 정보보안 관리직 1,504명, 정보보안 영업직이 367명 순으로 높게 나타났다.

[표 4-17] 정보보안산업 직종별 인력 현황

(2018년 12월 현재)

구분	세부 분류	4년 미만	4년 이상 7년 미만	7년 이상 11년 미만	11년 이상 15년 미만	15년 이상	합계 (명)	비중 (%)
정보보안 연구 및 개발직	암호 및 인증 기술, 시스템 및 네트워크 기술, 응용기술 및 서비스	1,877	1,197	793	451	279	4,597	34.4
정보보안 관리직	정보시스템 관리	626	1,017	692	322	125	2,782	20.8
	정보보안 컨설팅	336	665	431	187	77	1,696	12.7
	정보보안 관제	542	588	505	239	57	1,931	14.4
정보보안 영업직	정보보안 마케팅	367	382	423	519	242	1,933	14.4
기타 정보보안 관련직	정보시스템 감리 및 인증, 정보보안 교육, 기타	89	59	71	107	113	439	3.3
합 계		3,837	3,908	2,915	1,825	893	13,378	100.0

나. 매출액 규모별 현황

매출액 규모별로 살펴보면, 100억 이상 기업에서 전체 15년 이상 기술자 893명 중 697명을 보유하고 있으며, 10억 이상 50억 미만 기업이 98명의 15년 이상 기술자를 보유하고 있는 것으로 조사되었다.

11년 이상 15년 미만 기술자의 경우, 100억 이상 기업이 전체 11년 이상 15년 미만 기술자 1,825명 중 1,423명을 보유하고 있으며, 10억 이상 50억 미만 기업체가 190명, 10억 미만 기업이 22명의 11년 이상 15년 미만 기술자를 보유하고 있는 것으로 조사되었다.

7년 이상 11년 미만 기술자는 총 2,915명으로 이 중 2,105명이 100억 이상 기업에서 종사하고 있으며, 10억 이상 50억 미만 기업에 308명, 10억 미만 기업에 71명이 종사하고 있는 것으로 조사되었다.

4년 이상 7년 미만 기술자는 총 3,908명으로 이 중 2,837명이 100억 이상 기업에 종사하고 있으며, 352명이 10억 이상 50억 미만 기업에 종사하고, 116명이 10억 미만 기업에 종사하고 있는 것으로 조사되었다.

4년 미만 기술자는 총 3,837명으로 이 중 2,921명이 100억 이상 기업에 종사하고 있으며, 310명이 10억 이상 50억 미만 기업에 종사하고, 84명이 10억 미만 기업에 종사하고 있는 것으로 조사되었다.

[표 4-18] 정보보안산업 매출액 규모별 인력 현황

(2018년 12월 현재)

매출액 규모	4년 미만	4년 이상 7년 미만	7년 이상 11년 미만	11년 이상 15년 미만	15년 이상	합계(명)
10억 미만	84	116	71	22	10	303
10억~50억 미만	310	352	308	190	98	1,258
50억~100억 미만	522	603	431	190	88	1,834
100억 이상	2,921	2,837	2,105	1,423	697	9,983
합 계	3,837	3,908	2,915	1,825	893	13,378

다. 종사자 규모별 현황

종사자 규모별로 살펴보면, 15년 이상 기술자 892명 중 200인 이상 기업에 458명이 종사하고 있는 것으로 조사되었으며 20인 이상 100인 미만 기업에 224명, 100인 이상 200인 미만 기업에 185명이 종사하고 있는 것으로 조사되었다.

11년 이상 15년 미만 기술자의 경우, 총 1,826명 중 200인 이상 기업체에 909명이 종사하고 있으며, 20인 이상 100인 미만 기업체에 456명, 100인 이상 200인 미만 기업체에 389명이 종사하고 있는 것으로 조사되었다.

7년 이상 11년 미만 기술자의 경우, 총 2,915명 중 200인 이상 기업체에 1,480명이 종사하고 있으며, 20인 이상 100인 미만 기업체에 699명, 100인 이상 200인 미만 기업체에 583명이 종사하고 있는 것으로 조사되었다.

4년 이상 7년 미만 기술자의 경우, 총 3,908명 중 200인 이상 기업체에 2,052명이 종사하고 있으며, 100인 이상 200인 미만 기업체에 754명, 20인 이상 100인 미만 기업체에 865명, 20인 미만 기업체에 237명이 종사하고 있는 것으로 조사되었다.

4년 미만 기술자의 경우, 총 3,837명 중 200인 이상 기업체에 2,091명이 종사하고 있으며, 100인 이상 200인 미만 기업체에 783명, 20인 이상 100인 미만 기업체에 795명, 20인 미만 기업체에 168명이 종사하고 있는 것으로 조사되었다.

[표 4-19] 정보보안산업 종사자 규모별 인력 현황

(2018년 12월 현재)

종사자 규모	4년 미만	4년 이상 7년 미만	7년 이상 11년 미만	11년 이상 15년 미만	15년 이상	합계(명)
20인 미만	168	237	153	72	25	655
20인-100인 미만	795	865	699	456	224	3,039
100인-200인 미만	783	754	583	389	185	2,694
200인 이상	2,091	2,052	1,480	908	459	6,990
합 계	3,837	3,908	2,915	1,825	893	13,378

라. 기업 형태별 현황

정보보안 기업의 경우 기업 형태별 기술 등급별 종사자 수를 살펴보면 15년 이상 기술자 892명 중 468명이 일반기업에 종사하고 있으며, 424명이 벤처기업에 종사하고 있다.

11년 이상 15년 미만 기술자의 경우, 1,826명 중 1,132명이 일반기업에 종사하고 있으며 694명이 벤처기업에 종사하고 있다.

7년 이상 11년 미만 기술자의 경우, 2,915명 중 1,982명이 일반기업에 종사하고 있으며, 933명이 벤처기업에 종사하고 있는 것으로 조사되었다.

4년 이상 7년 미만 기술자의 경우, 총 3,908명 중 2,778이 일반기업에 종사하고 있으며, 1,130명이 벤처기업에 종사하고 있는 것으로 조사되었다.

4년 미만 기술자의 경우, 총 3,837명 중 2,628명이 일반기업에 종사하고 있으며, 1,209명이 벤처기업에 종사하고 있는 것으로 조사되었다.

[표 4-20] 정보보안산업 기업 형태별 인력 현황

(2018년 12월 현재)

기업형태	4년 미만	4년 이상 7년 미만	7년 이상 11년 미만	11년 이상 15년 미만	15년 이상	합계(명)
일반기업	2,628	2,778	1,982	1,132	468	8,988
벤처기업	1,209	1,130	933	693	425	4,390
합 계	3,837	3,908	2,915	1,825	893	13,378

3 채용 현황

가. 분야별 채용 현황

2019년도 정보보안 기업의 분야별 인력 채용 현황을 살펴보면, 신입직으로 총 803명을 채용하였고, 경력직으로 총 1,003명을 채용한 것으로 조사되었다.

[표 4-21] 정보보안산업 분야별 인력 채용 현황

(2019년 예상)

	2019년 채용
신입	803
경력	1,003
합계	1,806

나. 매출액 규모별 채용 현황

매출액 규모별로 인력채용 현황을 살펴보면 1,806명 중 100억 이상 기업이 1,150명을 채용하였으며, 50억 이상 100억 미만 기업이 313명, 10억 이상 50억 미만 기업이 279명, 10억 미만 기업이 64명을 채용한 것으로 조사되었다.

채용경력별로 살펴보면, 매출액 규모별 모든 구간에서 신입직 보다는 경력직을 더 많이 채용한 것으로 조사되었다.

[표 4-22] 정보보안 매출액 규모별 인력 채용 현황

(2019년 예상)

매출액 규모	2019년(채용)		합계(명)
	신입	경력	
10억 미만	24	40	64
10억-50억 미만	138	141	279
50억-100억 미만	143	170	313
100억 이상	498	652	1,150
합계	803	1,003	1,806

다. 종사자 규모별 채용 현황

종사자 규모별 인력 채용 현황을 살펴보면, 20인 이상 100인 미만 기업체에서 520명을 채용하였으며, 200인 이상 기업체에서 779명, 100인 이상 200인 미만 기업체에서 337명을 채용한 것으로 조사되었다.

[표 4-23] 정보보안 종사자 규모별 인력채용 현황

(2019년 예상)

종사자 규모	2019년(채용)		합계(명)
	신입	경력	
20인 미만	79	91	170
20인~100인 미만	249	271	520
100인~200인 미만	152	185	337
200인 이상	323	456	779
합계	803	1,003	1,806

라. 기업 형태별 채용 현황

기업형태별 인력 채용 현황을 살펴보면, 총 1,806명 중 1,192명을 일반기업이 채용한 것으로 조사되었으며 나머지 614명을 벤처기업이 채용한 것으로 조사되었다. 일반기업과 벤처기업 모두 경력직을 상대적으로 많이 채용한 것으로 조사되었다.

[표 4-24] 정보보안 기업형태별 인력채용 현황

(2019년 예상)

기업 형태	2019년(채용)		합계(명)
	신입	경력	
일반기업	523	669	1,192
벤처기업	280	334	614
합계	803	1,003	1,806

4 채용 계획

정보보안관련 기업체의 2020년 신규 예정 채용인력은 총 1,334명으로 조사되었다. 신입직보다는 경력직의 채용 비중이 더 높은 것으로 조사되었다.

[표 4-25] 정보보안산업 분야별 채용계획

(2020년 예상)

	2020년(채용 계획)
신입	625
경력	709
합계	1,334

채용 예정 인원 역시 매출액 규모가 가장 큰 100억 이상 기업에서 942명을 채용 예정인 것으로 조사되었으며, 종사자 규모별로는 200인 이상 기업에서 724명을 채용할 예정인 것으로 조사되었다.

기업형태별로 살펴보면, 일반기업이 923명을 채용할 예정이며 벤처기업이 411명을 채용할 예정인 것으로 조사되었다.

[표 4-26] 정보보안 기업 특성별 채용 계획

(2020년 예상)

구분		계획 인원 (명)
매출액 규모	10억 미만	42
	10억~50억 미만	224
	50억~100억 미만	126
	100억 이상	942
종사자 규모	20인 미만	141
	20인~100인 미만	273
	100인~200인 미만	196
	200인 이상	724
기업형태	일반기업	923
	벤처기업	411

제5절 기술개발 및 동향

1 자체기술연구소 및 연구개발 전담부서 운영

정보보안기업의 기술개발 관련 자체기술연구소 및 전담부서 운영 현황을 조사한 결과, 기업부설연구소를 운영하는 기업은 288개 60.9%, 연구개발 전담부서를 운영하는 기업은 141개 29.8%로 조사되었다. 기업부설연구소와 연구개발 전담부서를 모두 운영하지 않는 기업은 44개 9.3%로 나타났다.

기업부설연구소를 운영하는 288개 기업 중 20인 이상 100인 미만의 기업이 121개였으며, 20인 미만의 기업이 98개 기업으로 나타났다.

[표 4-27] 정보보안 기업 자체기술연구소 및 전담부서 운영 현황

(단위: 개, %)

구분	종사자 기준				운영현황	
	20인 미만	20인 이상-100인 미만	100인 이상-200인 미만	200인 이상	합계	비율(%)
기업부설연구소 운영	98	121	41	28	288	60.9
연구개발전담부서 운영	53	67	9	12	141	29.8
없음	30	12	2	0	44	9.3
총 기업수	181	200	52	40	473	100.0

2 연도별 기술개발 투자액 현황

정보보안 기업의 연도별 기술개발 투자액 현황 및 향후 전망을 조사한 결과 2018년도 전체 투자액 규모가 있는 기업은 모두 153개이며, 기술연구 개발비의 경우 평균 1,925.6백만원, 연구개발 투자액 규모는 150개 기업이 평균 1,906.9백만원을 투자한 것으로 나타났다.

2019년도 전체 투자액이 있는 기업은 158개 평균 2,217.9백만원, 연구개발 투자액 규모는 157개 기업 평균 1,977.7백만원을 투자할 계획인 것으로 조사되었다.

기업당 기술개발에 투자하는 평균 금액은 해마다 증가하고 있지만, 이를 매출액 대비 비중으로 환산해보면 2018년도 14.1%, 2019년도 13.7% 등 14% 전후 수준으로 예상된다.

[표 4-28] 정보보안 기업 연도별 기술개발 투자액 현황

(단위 : 개, 백만원, %)

구분	2018년		2019년(E)		2020년(E)	
	기업수	투자액평균	기업수	투자액평균	기업수	투자액평균
전체 투자액 (연구개발/건물/ 기계/설비 등)	153	1,925.6	158	2,217.9	163	2,193.6
연구개발 투자액	150	1,906.9	157	1,977.7	161	1,920.7
매출 대비 투자 비율(%)	14.1		13.7		13.9	

3 기술개발시 애로사항

정보보안 기업들의 기술개발 시 애로사항으로 기술개발 인력 확보 및 유지가 40.7%로 가장 높게 나타났다. 다음으로 자금조달이 27.2%의 순으로 조사 되었다. 그 외에도 기술정보 부족 및 획득 곤란 9.6%, 신기술의 짧은 수명주기 8.3% 등으로 조사되었다.

[표 4-29] 정보보안 기술개발시 애로사항(복수응답)

(단위 : %)

구분	비율(%)
기술개발 인력 확보 및 유지	40.7
자금조달	27.2
기술정보 부족 및 획득 곤란	9.6
연구 설비 기자재 부족	8.0
신기술의 짧은 수명주기	8.3
기타	6.2
합계	100.0

4 지식재산권 보유 현황

정보보안 관련 지식재산권 보유현황을 조사한 결과, 현재 보유하고 있거나 출원 중인 지식재산권은 2,546건으로 나타났다. 이를 구체적으로 살펴보면 현재 보유중인 지식재산권이 2,120건, 출원 중인 지식재산권이 426건인 것으로 조사되었다.

현재 보유중인 정보보안 지식재산권을 보면 특허권 1,391건(65.6%), 실용신안권 201건(9.5%), 의장권 61건(2.9%), 상표권 467건(22.6%)으로 조사되었다.

현재 출원 중인 정보보안 지식재산권은 특허권 345건(81.0%), 실용신안권 20건(4.7%), 상표권 61건(14.3%)으로 조사되었다.

한편, 해외 특허의 경우 69개 기업이 해외 특허를 보유하고 있으며, 총 181건으로 기업 당 평균 2.6건을 보유하고 있었다. 현재 출원 중인 기업은 15개 기업으로 총 33건을 출원 중이며, 기업당 평균 2.2건을 출원 중에 있는 것으로 조사되었다.

[표 4-30] 정보보안 지식재산권 보유 현황

(단위 : 건, %)

구분		현재 보유		현재 출원 중	
		건수	비율(%)	건수	비율(%)
지식재산권	특허권	1,391	65.6	345	81.0
	실용신안권	201	9.5	20	4.7
	의장권	61	2.9	0	0.0
	상표권	467	22.6	61	14.3
합계		2,120	100.0	426	100.0

[표 4-31] 정보보안 해외특허 보유 현황

(단위 : 개, %, 건)

건수	보유기업 수	보유기업 비율(%)	총 건수	평균 건수
현재 보유	69	14.6	181	2.6
현재 출원 중	15	3.2	33	2.2

5 매출규모별 제품 비중

매출규모별 제품비중을 조사한 결과, 자사제품 판매 비율이 81.1%, 국내 타사 제품 유통비율이 14.1%, 외산 제품 유통 비율은 4.8%로 조사되었다.

[표 4-32] 정보보안 매출규모별 제품비중

(단위 : %)

구분	비중
자사제품 판매	81.1
국내 타사제품 유통	14.1
외산제품 유통	4.8
합계	100.0

6 사업추진에 따른 하도급, 유지보수 및 라이선스 요율 정도

사업 추진에 따른 하도급, 유지보수 및 라이선스 요율 정도는 공공사업의 하도급 비율은 39.8%, 연간 유지관리(유지보수) 요율은 9.6%인 것으로 조사되었으며, 라이선스 요율은 16.2%인 것으로 조사되었다. 공공사업의 경우 민간사업인 경우에 비하여 하도급 비율은 높고, 유지보수 요율은 낮은 것으로 나타났다. 보안성지속서비스 요율의 경우, 아직까지는 공공사업, 민간사업 모두 현장에서 활성화되지는 않은 것으로 파악되었다.

[표 4-33] 사업추진에 따른 하도급, 유지보수 및 라이선스 요율

(단위 : %)

구분	공공사업	민간사업
하도급 비율	39.8	37.5
연간 유지관리(유지보수) 요율	9.6	9.9
보안성지속서비스 요율	0	0
라이선스 요율	16.2	18.0

7 주요 경쟁 요소

기술/품질, 인지도, 마케팅, 가격, 입지적 유리 등 6개 항목에 대해 주요 경쟁 요소를 조사한 결과 기술, 품질이 주요 경쟁 요소라는 응답이 50.6%로 가장 높게 나타났다.

[표 4-34] 정보보안 주요 경쟁 요소(복수응답)

구분	빈도(개)	비율(%)
기술, 품질	162	50.6
가격	47	14.7
마케팅	54	16.9
인지도	50	15.6
입지적 유리	7	2.2
기타	0	0.0
합계	320	100.0

8 기업 경영/기술정보 수집 경로

정보보안 기업들은 경영/기술 정보를 동종업체, 세미나/학회, 미디어, 업종단체/협회, 협력업체, 정부 및 공공기관 등 다양한 채널을 통해 수집하는 것으로 조사되었다. 중복응답을 포함하여 총 278개 응답 가운데 제품/서비스 협력업체 33.1%, 관련 업종단체/협회 18.7%, 정부 및 공공기관 16.2%, 고객(납품 모기업) 11.1%인 것으로 조사되었다.

[표 4-35] 정보보안 경영/기술정보 수집 경로(복수응답)

구분	빈도(개)	비율(%)
대학/연구소	28	10.1
정부 및 공공기관	45	16.2
고객(납품 모기업)	31	11.1
제품/서비스 협력업체	92	33.1
관련 업종단체/협회	52	18.7
컨설팅업체	9	3.2
금융기관	2	0.7
동종업체간 교류	18	6.5
기타	1	0.4
합계	278	100.0

9 시장 경쟁 및 산업 동향 동의 수준

성장성의 경우 신기술, 신제품의 지속적 출현에 대해서는 동의정도가 상대적으로 높게 나타났다. 경쟁성의 경우 가격 경쟁의 치열, 신기술 습득, 시장 규모의 포화상태에 대해서는 동의정도가 높은 것으로 조사되었다. 기술력의 경우, 국내시장의 기술력 낮음, 통합솔루션 제공 미약에 있어서는 상대적으로 동의정도가 낮았다.

[표 4-36] 정보보안 시장 경쟁 및 산업 동향 동의 수준

(단위 : 점, 5점 만점)

구분	시장 상황 및 산업 동향	동의 수준
성장성	신기술, 신제품이 지속적으로 출현하고 있다.	3.75
	기업 이익을 안정적으로 확보할 수 있다.	3.51
	기술 변화의 예측이 어느 정도 가능하다.	3.57
경쟁성	시장 규모가 포화상태이다	3.82
	가격 경쟁이 치열하다.	3.93
	경쟁자 전략의 예측이 가능하다.	3.60
	신기술 습득을 위한 경쟁이 치열하다.	3.74
	국산과 외산의 경쟁이 증가하고 있다.	3.66
기술력	국내시장 기술력이 낮다.	2.69
	통합솔루션 제공이 미약하다.	2.77
기타	자금상황이 어려운 편이다.	3.02

10 시장 확대를 위한 정부지원 필요 부분

시장 확대를 위한 정부 지원이 필요한 부분으로 기술개발 지원 34.1%로 가장 높게 나타났으며, 다음으로 전문인력 양성 18.9%, 자금지원 및 세제혜택 15.8%, 공공부문의 시장수요 창출 10.8% 등의 순으로 높게 조사되었다.

[표 4-37] 정보보안 시장 확대를 위한 정부 지원 필요 사항(복수응답)

구 분	빈도(개)	비율(%)
전문인력 양성	61	18.9
기술개발 지원	110	34.1
기술이전의 활성화	22	6.8
법/제도 제 개정	21	6.5
공공부문의 시장수요 창출	35	10.8
소비촉진/투자활성화	14	4.3
자금지원 및 세제혜택	51	15.8
해외지원 사업 확대	7	2.2
기타	2	0.6
합계	323	100.0

11 해외 진출시 애로사항

해외 진출시 애로사항으로 판로개척이 3.17점으로 가장 높게 인식되고 있었으며, 세계경제 불안 및 경기 둔화 3.14점, 현지 법 및 제도 3.08점, 관세·통관절차 부담 2.98점, 환율하락에 따른 채산성 악화 2.97점 등의 순으로 높게 나타났다.

[표 4-38] 정보보안산업 해외 진출시 애로사항

(단위 : 점, 5점 만점)

애로사항	수준
환율하락에 따른 채산성 악화	2.97
자금유동성 부족	2.88
현지 법 및 제도	3.08
판로개척	3.17
관세·통관절차 부담	2.98
지적재산권 보호역량 부족	2.93
국제표준 및 인증획득	2.95
세계경제 불안 및 경기둔화	3.14
인력 부족	2.95

2019

국내 정보보호산업
실태조사



제5장 물리보안산업 현황

제1절 기업 현황	87
제2절 매출 현황	92
제3절 수출 현황	108
제4절 인력 및 채용 현황	118
제5절 기술개발 및 동향	126

5장

물리보안산업 현황

제1절 기업 현황

1 지역별 현황

물리보안 관련 기업 소재지의 경우 621개 기업 가운데 191개 기업(30.8%)이 서울에 소재하고 있는 것으로 조사되었다. 경기 242개(39.0%), 인천 30개(4.8%), 대전 23개(3.7%) 순으로 조사되었다. 서울, 경기 등 수도권에 물리보안 기업의 74.6%가 집중되어 있는 것으로 나타났다.

[표 5-1] 물리보안 기업의 지역별 분포

지역	기업수(개)	비율(%)
서울	191	30.8
경기	242	39.0
대전	23	3.7
부산	18	2.9
대구	18	2.9
광주	16	2.6
전남	8	1.3
경남	16	2.6
경북	19	3.1
인천	30	4.8
제주	2	0.3
충남(세종)	7	1.1
충북	5	0.8
강원	10	1.6
울산	5	0.8
전북	11	1.8
합계	621	100.0

2 기업 형태별 현황

물리보안 관련 기업의 기업 형태별 현황을 살펴보면 일반기업이 344개(55.4%), 벤처기업이 277개(44.6%)인 것으로 조사되었다.

[표 5-2] 물리보안 기업 형태별 현황

구분	일반	벤처	합계
기업수(개)	344	277	621
비율(%)	55.4	44.6	100.0

3 상장 유무 현황

물리보안 관련 기업의 상장 유무별 현황을 살펴보면 비상장 기업이 586개(94.4%), 코스닥 상장 기업이 31개(5.0%), 유가증권 상장 기업이 2개(0.3%), 코넥스 상장 기업이 2개(0.3%)인 것으로 조사되었다.

[표 5-3] 물리보안 기업 상장 유무별 현황

구분	비상장	코스닥	유가증권	코넥스	합계
기업수(개)	586	31	2	2	621
비율(%)	94.4	5.0	0.3	0.3	100

4 설립연도별 현황

물리보안 관련 기업의 설립연도별 현황을 살펴보면 2000년 이전 설립 기업이 133개(21.4%), 2000년 이후 2005년 이전 설립 기업이 153개(24.6%), 2005년 이후 2010년 이전 설립 기업이 133개(21.4%), 2010년 이후 설립 기업이 202개(32.5%)인 것으로 조사되었다.

[표 5-4] 물리보안 기업 설립연도별 현황

구분	2000년 이전	2000년 이후- 2005년 이전	2005년 이후- 2010년 이전	2010년 이후	합계
기업수(개)	133	153	133	202	621
비율(%)	21.4	24.6	21.4	32.5	100.0

5 자본금 규모별 현황

물리보안 관련 기업의 자본금 규모별 현황을 살펴보면 자본금 10억 미만 기업이 458개(73.8%), 10억 이상 50억 미만 기업이 125개(20.1%), 50억 이상 100억 미만 기업이 28개(4.5%), 100억 이상 기업이 10개(1.6%)인 것으로 조사되었다.

[표 5-5] 물리보안 기업 자본금 규모별 현황

구분	10억 미만	10억 이상- 50억 미만	50억 이상- 100억 미만	100억 이상	합계
기업수(개)	458	125	28	10	621
비율(%)	73.8	20.1	4.5	1.6	100.0

6 종사자 규모별 현황

물리보안 관련 기업의 종업원 규모별 현황을 살펴보면 20인 미만 기업이 338개(54.5%), 20인 이상 100인 미만 기업이 212개(34.1%), 100인 이상 200인 미만이 33개(5.3%), 200인 이상인 기업은 31개(6.1%)인 것으로 조사되었다.

[표 5-6] 물리보안 기업 종사자 규모별 현황

구분	20인 미만	20인 이상- 100인 미만	100인 이상- 200인 미만	200인 이상	합계
기업수(개)	338	212	33	38	621
비율(%)	54.5	34.1	5.3	6.1	100.0

7 취급 품목별 현황

물리보안 관련 기업이 취급하는 품목을 중분류로 구분하여 이에 포함된 제품 중 어느 하나라도 취급하면 판매에 기여하는 것으로 보고 중복으로 계수하여 취급 품목별로 정리한 결과는 [표 5-7]과 같다.

물리보안 시스템 개발 및 공급을 83.6%의 기업이 취급하며, 물리보안 관련 서비스를 취급하는 기업은 전체의 16.4%인 것으로 조사되었다.

제품별 취급 기업 수를 살펴보면 CCTV 카메라 부품 20.3%, 보안용 카메라 제조 15.5%, 물리보안 주변장비 10.9%, 보안용 저장장치 제조 8.9%, 물리보안 솔루션 7.2%, 출입통제 장비 제조 6.1%, 기타 제품 6.0%, 경보/감시 장비 제조 5.1%, 생체인식 보안시스템 제조 3.7%로 조사되었다.

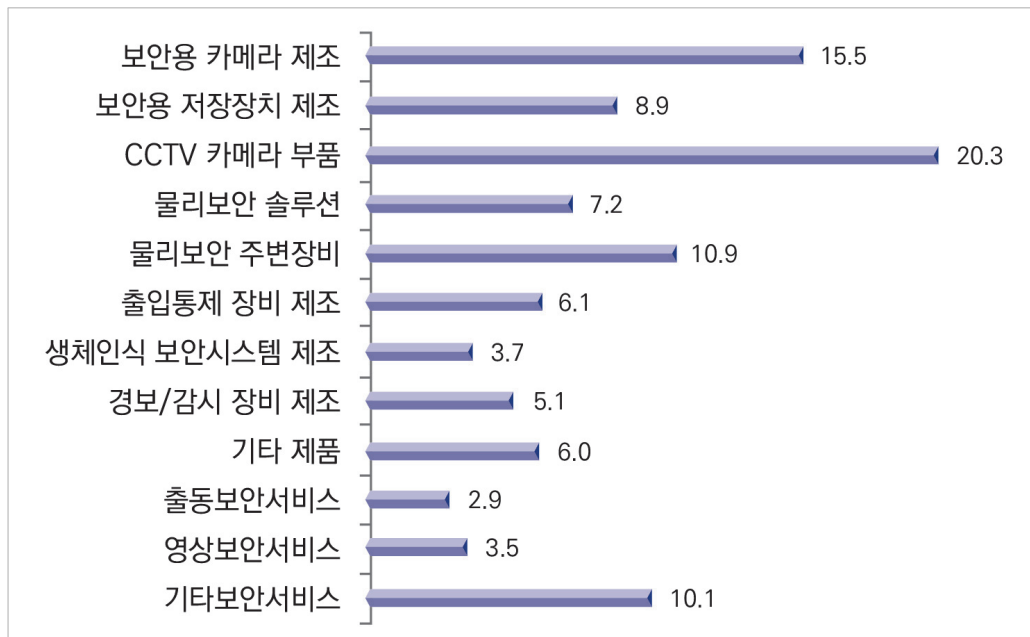
물리보안 관련 서비스의 경우는 기타보안서비스 10.1%, 영상보안서비스 3.3%, 출동보안서비스 2.9%가 취급되고 있는 것으로 조사되었다.

[표 5-7] 물리보안 기업 중분류 품목별 취급 기업 현황

구분		기업수(개)	비율(%)
물리보안 시스템 개발 및 공급	보안용 카메라 제조	152	15.5
	보안용 저장장치 제조	87	8.9
	CCTV 카메라 부품	199	20.3
	물리보안 솔루션	71	7.2
	물리보안 주변장비	107	10.9
	출입통제 장비 제조	60	6.1
	생체인식 보안시스템 제조	36	3.7
	경보/감시 장비 제조	50	5.1
	기타 제품	59	6.0
	소계	821	83.6
물리보안 관련 서비스	출동보안서비스	28	2.9
	영상보안서비스	34	3.5
	기타보안서비스	99	10.1
	소계	161	16.4
합계		982	100.0

[그림 5-1] 물리보안 기업 중분류 품목별 취급 기업 현황

(단위 : %)



제2절 매출 현황

1 전체 매출 현황

가. 대분류 현황

2019년 물리보안 기업의 매출은 7,279,550백만원으로 2018년 7,034,918백만원 대비 3.5% 성장한 것으로 조사되었다.

강력범죄 예방 및 치안문제 해결, 재난·화재 감시 등 국민의 생명과 재산을 보호하기 위한 수요와 건물 및 공공 시설물 보안 및 관리를 위한 수요가 증가하면서 산업이 지속적으로 성장하고 있다.

또한 2010년 ‘주택건설기준 등에 관한 규정’에서의 300세대 이상 공동주택의 CCTV 설치 의무화, 2012년 행정안전부의 ‘CCTV 종합대책’, 지자체의 ‘통합관제센터 구축사업 본격화’ 등 정부 차원의 지원이 국내 물리보안산업이 지속적으로 성장하는데 주요 요인으로 작용하였다.

그리고 물리보안 제품의 네트워크화, 신규 서비스(가정 및 유아안심서비스), 기존 노후장비(저화소 카메라, 아날로그 영상장비)의 교체수요 등도 물리보안산업이 지속적으로 성장하는데 한축을 담당하는 것으로 분석된다.

[표 5-8] 물리보안산업 대분류 매출 현황

(단위 : 백만원, %)

구분	2018년	2019년(E)	증감율(%)
물리보안 시스템 개발 및 공급	4,421,928	4,599,723	4.0
물리보안 관련 서비스	2,612,990	2,679,827	2.6
합계	7,034,918	7,279,550	3.5

나. 중분류 현황

물리보안산업의 중분류별 매출을 살펴보면, 물리보안 시스템 개발 및 공급은 보안용 카메라 제조, 보안용 저장장치 제조, CCTV 카메라 부품분야의 매출 비중이 높으며, 물리보안 관련 서비스는 출동보안 서비스, 기타보안 서비스 분야의 매출 비중이 높은 것으로 조사되었다.

물리보안 시스템 개발 및 공급에서는 물리보안 솔루션 10.6%, 생체인식 보안시스템 제조 7.4%, 물리보안 관련 서비스에서는 기타보안서비스 10.6% 증가한 것으로 조사되었다.

[표 5-9] 물리보안산업 중분류 매출 현황

(단위 : 백만원, %)

구분		2018년	2019년(E)	증감율(%)
물리보안 시스템 개발 및 공급	보안용 카메라 제조	1,106,250	1,171,005	5.9
	보안용 저장장치 제조	907,487	923,263	1.7
	CCTV 카메라 부품	484,766	506,379	4.5
	물리보안 솔루션	378,902	419,198	10.6
	물리보안 주변장비	161,576	164,153	1.6
	출입통제 장비 제조	499,455	505,019	1.1
	생체인식 보안시스템 제조	293,378	315,218	7.4
	경보/감시 장비 제조	220,715	221,179	0.2
	기타 제품	369,398	374,307	1.3
	소계	4,421,927	4,599,723	4.0
물리보안 관련 서비스	출동보안서비스	1,726,210	1,727,972	0.1
	영상보안서비스	401,777	415,647	3.5
	기타보안서비스	485,004	536,208	10.6
	소계	2,612,991	2,679,827	2.6
합계		7,034,918	7,279,550	3.5

다. 업종별 매출 현황

물리보안 시스템 개발 및 공급 분야의 업종별 매출비중은 일반업종 53.9%의 가장 높은 매출 비중을 보였고, 다음으로 공공업종 33.1%, 금융업종 13.0% 순으로 나타났다. 물리보안 관련 서비스의 업종별 매출비중에서는 일반업종이 가장 많은 50.8%의 매출 비중을 보였으며, 공공업종 36.2%, 금융업종 13.0%로 각각 조사되었다.

[표 5-10] 물리보안산업 업종별(수요처별) 매출 현황

(단위 : %)

구분	업종(수요처)			
	공공	금융	일반	합계
물리보안 시스템 개발 및 공급	33.1	13.0	53.9	100.0
물리보안 관련 서비스	36.2	13.0	50.8	100.0

2 특성별 매출 현황

2019년 물리보안 총 매출액은 7,279,550백만원이며, 기업 특성별로 물리보안 총 매출액과 평균 매출액은 [표 5-11]와 같다.

[표 5-11] 기업 특성별 2019년 물리보안산업 매출 현황

(단위 : 백만원)

분류		매출액	평균액	분류		매출액	평균액
지역	서울	4,940,997	25,869	기업 형태	일반기업	5,823,680	16,929
	서울 외	2,338,553	5,438		벤처기업	1,455,869	5,256
설립 년도	2000년 이전	4,090,745	30,757	종사 자	20인 미만	616,266	1,823
	2000년 이후- 2005년 이전	700,974	4,582		20인-100인 미만	1,375,870	6,490
	2005년 이후- 2010년 이전	1,267,572	9,531		100인-200인 미만	1,213,521	36,773
	2010년 이후	1,220,259	6,041		200인 이상	4,073,893	107,208
상장 유무	비상장	3,795,703	6,477	자 본 금	10억 미만	1,053,215	2,300
	코스닥	3,055,624	98,569		10억-50억 미만	1,339,651	10,717
	유가증권	400,563	200,282		50억-100억 미만	1,677,484	59,910
	코넥스	27,660	13,830		100억 이상	3,209,200	320,920

서울지역에 위치한 물리보안 기업은 평균 매출액이 25,869백만원이었으며, 서울 외 지역에 위치한 물리보안 기업의 평균 매출액 5,438백만원으로 나타났다.

코스닥 기업의 평균 매출액은 98,569백만원으로 비상장 기업 6,477백만원과 차이를 보였으며, 기업 형태별로는 일반기업 16,929백만원, 벤처기업 5,256백만원으로 일반기업의 평균 매출액이 높은 것으로 조사되었다. 설립연도별로는 2000년 이전 기업이 30,757백만원, 2000년 이후 2005년 이전 기업이 4,582백만원, 2005년 이후 2010년 이전 기업이 9,531백만원, 2010년 이후 기업이 6,041백만원으로 2000년 이전 설립 기업의 평균 매출액이 높게 나타났다. 종사자 및 자본금 규모별로는 종사자 수가 증가할수록, 자본금 규모가 증가할수록 평균 매출액도 증가하는 것으로 조사되었다.

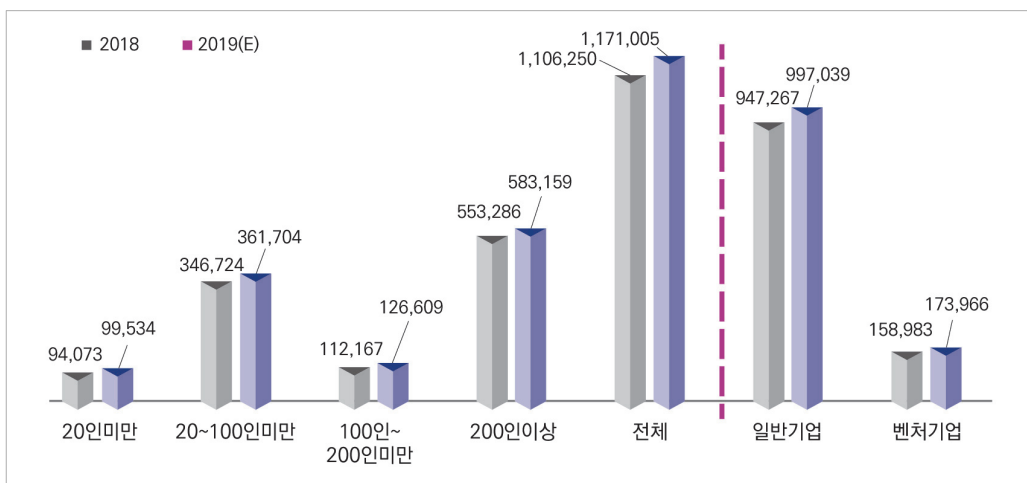
3 제품별 매출 현황

가. 보안용 카메라 제조

2018년 매출은 1,106,250백만원, 2019년 매출은 1,171,005백만원으로 5.9% 증가한 것으로 조사되었다. 보안용 카메라 제조는 종사자가 20인 이상 100인 미만 기업의 매출이 361,704백만원, 200인 이상 기업의 매출이 583,159백만원으로 종사자가 200인 이상인 기업에서 주로 판매되는 것으로 나타났다. 일반기업의 매출액은 997,039백만원이며, 벤처기업의 매출액은 173,966백만원으로 일반기업의 매출액이 벤처기업의 매출액보다 높은 것으로 나타났다.

[그림 5-2] 보안용 카메라 제조 매출 현황

(단위 : 백만원)

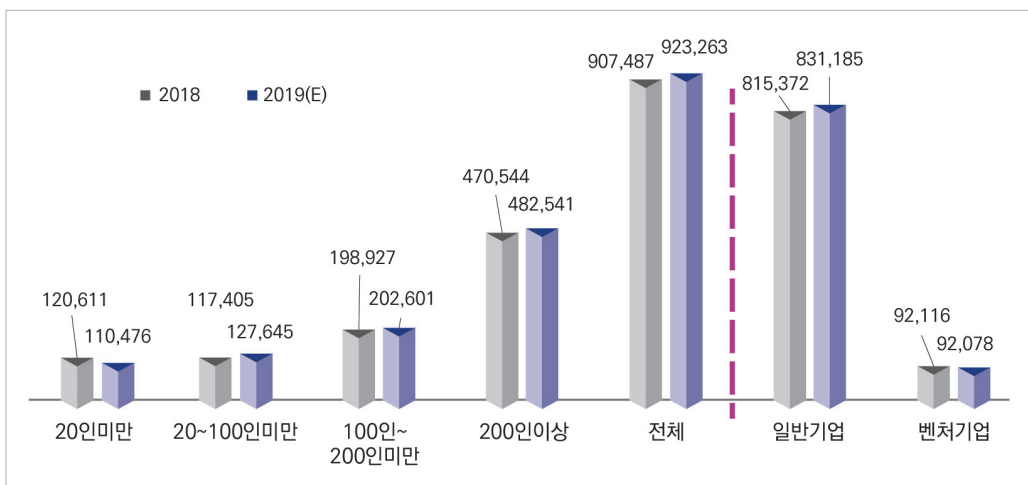


나. 보안용 저장장치 제조

2018년 매출은 907,487백만원, 2019년 매출은 923,263백만원으로 1.7% 증가한 것으로 조사되었다. 보안용 저장장치 제조는 종사자가 100인 이상 200인 미만 기업의 매출이 202,601백만원이며, 200인 이상 매출액이 482,541백만원으로 종사자가 200인 이상 기업에서 주로 판매되는 것으로 나타났다. 일반기업의 매출액은 831,185백만원이며, 벤처기업의 매출액은 92,078백만원으로 일반기업의 매출액이 벤처기업의 매출액보다 높은 것으로 나타났다.

[그림 5-3] 보안용 저장장치 제조 매출 현황

(단위 : 백만원)

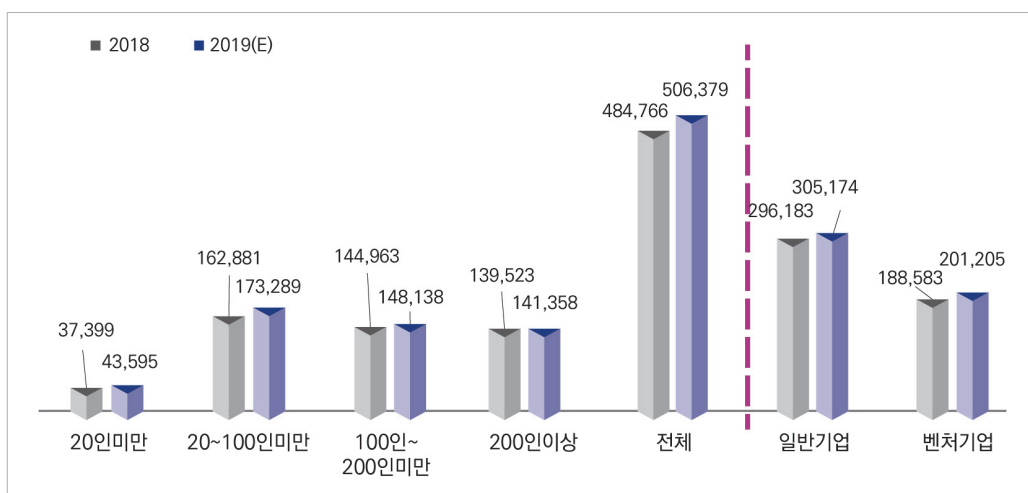


다. CCTV 카메라 부품

2018년 매출은 484,766백만원, 2019년 매출은 506,379백만원으로 4.5% 증가한 것으로 조사되었다. CCTV 카메라 부품은 종사자가 20인 이상 100인 미만 기업의 매출액이 173,289백만원, 100인 이상 200인 미만 기업의 매출액이 148,138백만원으로 나타났다. 일반기업의 매출액은 305,174백만원이며, 벤처기업의 매출액은 201,205백만원으로 일반기업의 매출액이 벤처기업의 매출액보다 높은 것으로 나타났다.

[그림 5-4] CCTV 카메라 부품 매출 현황

(단위 : 백만원)

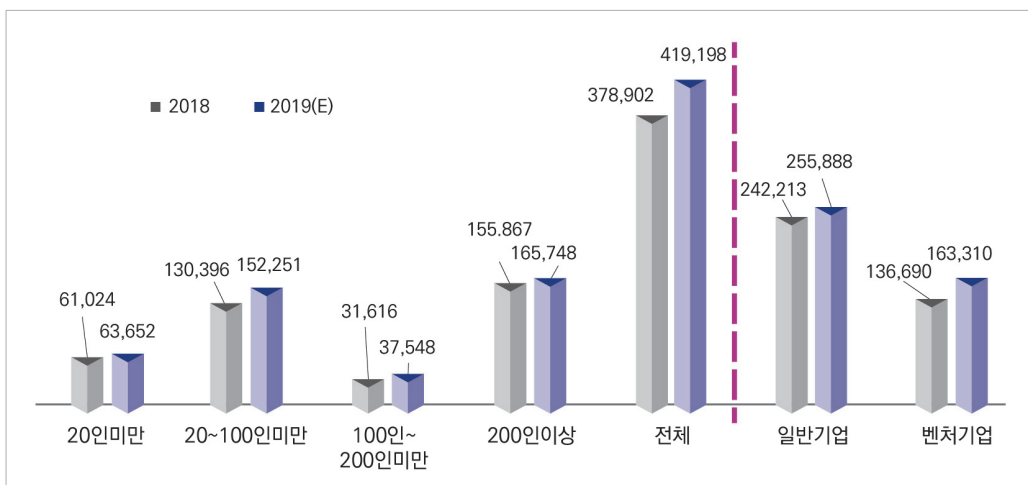


라. 물리보안 솔루션

2018년 매출은 378,902백만원, 2019년 매출은 419,198백만원으로 10.6% 증가한 것으로 조사되었다. 물리보안 솔루션은 종사자가 20인 이상 100인 미만 기업의 매출액이 152,251백만원이며, 200인 이상 기업의 매출액이 165,748백만원으로 종사자가 200인 이상 기업에서 주로 판매되는 것으로 나타났다. 일반기업의 매출액은 255,888백만원이며, 벤처기업의 매출액은 163,310백만원으로 일반기업의 매출액이 벤처기업의 매출액보다 높은 것으로 나타났다.

[그림 5-5] 물리보안 솔루션 매출 현황

(단위 : 백만원)

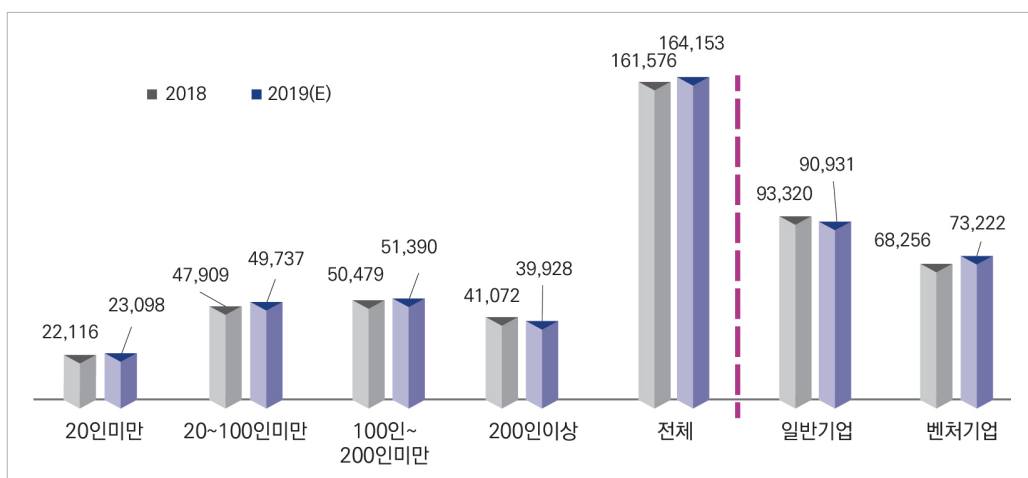


마. 물리보안 주변장비

2018년 매출은 161,576백만원, 2019년 매출은 164,153백만원으로 1.6% 증가한 것으로 조사되었다. 물리보안 주변장비는 종사자가 20인 이상 100인 미만 기업의 매출액이 49,737백만원이며, 100인 이상 200인 미만 기업의 매출액이 51,390백만원으로 종사자가 100인 이상 200인 미만 기업에서 주로 판매되는 것으로 나타났다. 일반기업의 매출액은 90,931백만원이며, 벤처기업의 매출액은 73,222백만원으로 일반기업의 매출액이 벤처기업의 매출액보다 높은 것으로 나타났다.

[그림 5-6] 물리보안 주변장비 제조 매출 현황

(단위 : 백만원)

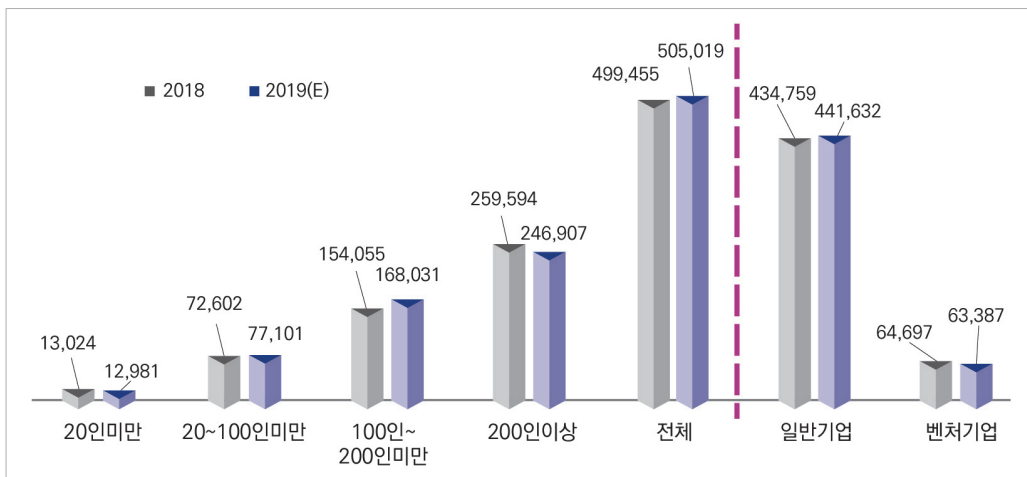


바. 출입통제 장비 제조

2018년 매출은 499,455백만원, 2019년 매출은 505,019백만원으로 1.1% 증가한 것으로 조사되었다. 출입통제 장비 제조는 종사자 수 100인 이상 200인 미만인 기업의 매출액이 168,031백만원, 200인 이상 기업의 매출액이 246,907백만원으로 조사되었다. 일반기업의 매출액은 441,632백만원이며, 벤처기업의 매출액은 63,387백만원으로 일반기업의 매출액이 벤처기업의 매출액보다 높은 것으로 나타났다.

[그림 5-7] 출입통제 장비 제조 매출 현황

(단위 : 백만원)

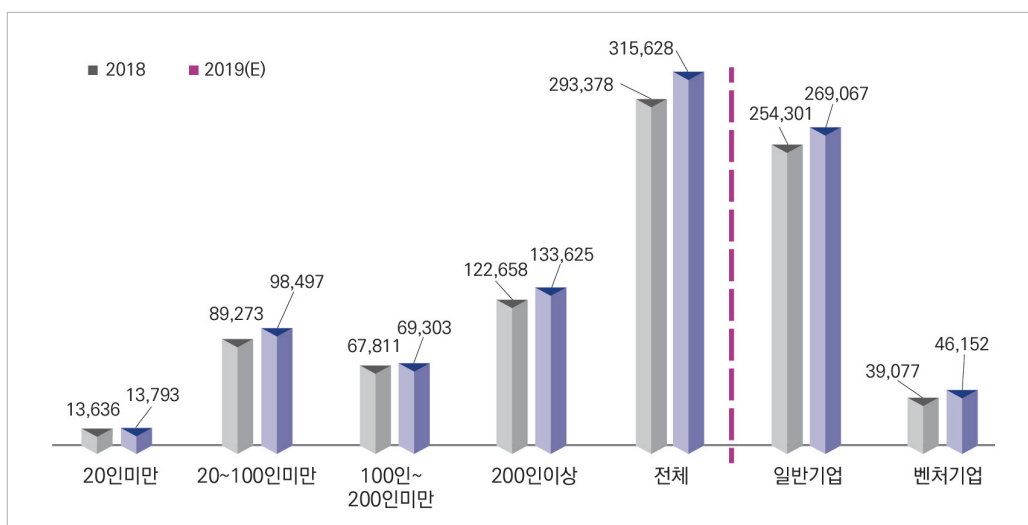


사. 생체인식 보안 시스템 제조

2018년 매출은 293,378백만원, 2019년 매출은 315,218백만원으로 7.4% 증가한 것으로 조사되었다. 생체인식 보안시스템 제조는 종사자 수가 20인 이상 100인 미만 기업의 매출은 98,497백만원이며, 200인 이상 매출액은 133,625백만원으로 종사자가 200인 이상인 기업에서 주로 판매되는 것으로 나타났다. 일반기업의 매출액은 269,067백만원이며, 벤처기업의 매출액은 46,152백만원으로 일반기업의 매출액이 벤처기업의 매출액보다 높은 것으로 나타났다.

[그림 5-8] 생체인식 보안 시스템 제조 매출 현황

(단위 : 백만원)

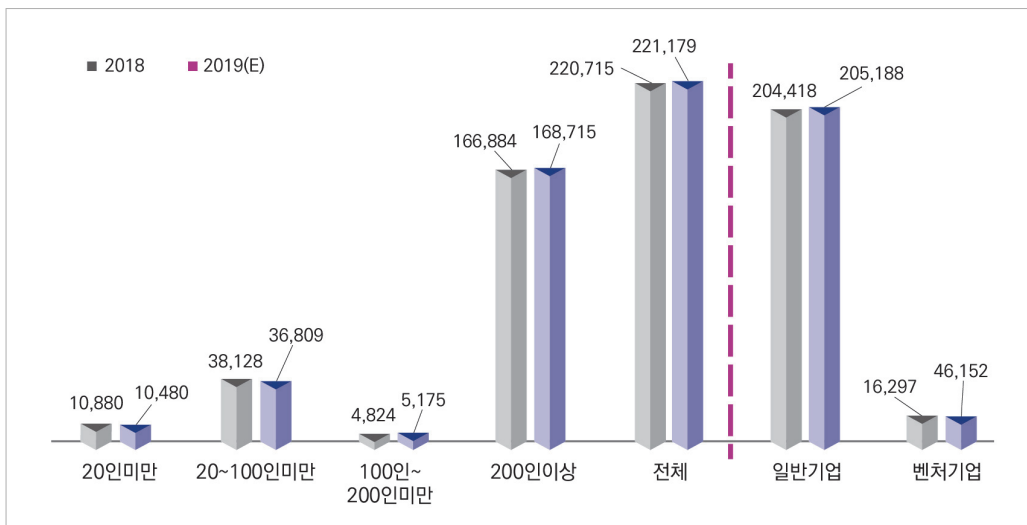


아. 경보/감시 장비 제조

2018년 매출은 220,715백만원, 2019년 매출은 221,179백만원으로 0.2% 증가한 것으로 조사되었다. 경보/감시장비 제조는 종사자 수 20인 이상 100인 미만 기업의 매출액이 36,809백만원, 200인 이상 기업의 매출액이 168,715백만원으로 주로 종사자가 200인 이상인 기업에서 판매되는 것으로 나타났다. 일반기업의 매출액은 205,188백만원이며, 벤처기업의 매출액은 15,992백만원으로 나타났다.

[그림 5-9] 경보/감시 장비 제조 매출 현황

(단위 : 백만원)

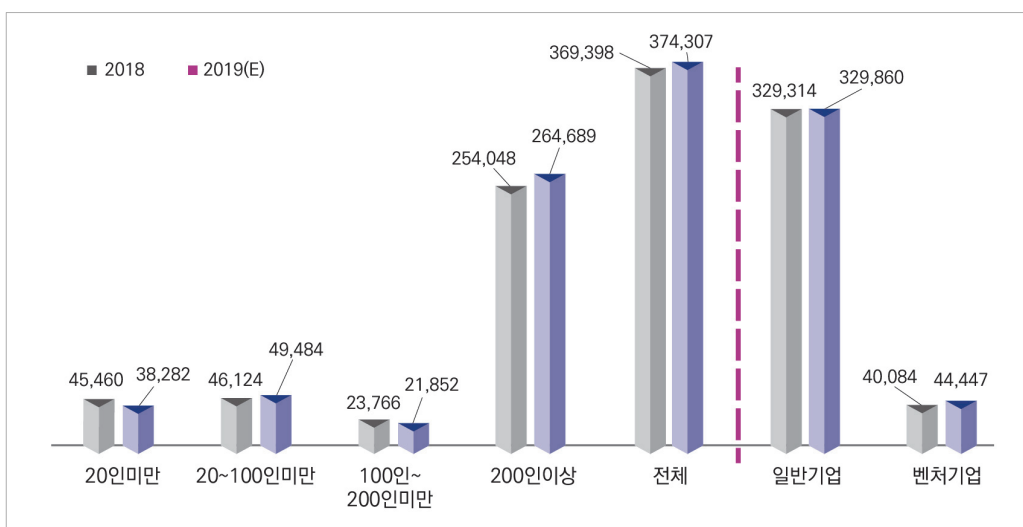


자. 기타 제품

2018년 매출은 369,398백만원, 2019년 매출은 374,307백만원으로 1.3% 증가한 것으로 조사되었다. 기타 제품은 종사자 수가 20인 이상 100인 미만 기업의 매출액이 49,484백만원, 200인 이상 기업의 매출액이 264,689백만원으로 주로 종사자가 200인 이상인 기업에서 판매되는 것으로 나타났다. 또한 일반기업의 매출액은 329,860백만원으로 벤처기업의 매출액 44,447백만원보다 매우 높은 것으로 나타났다.

[그림 5-10] 기타 제품 매출 현황

(단위 : 백만원)



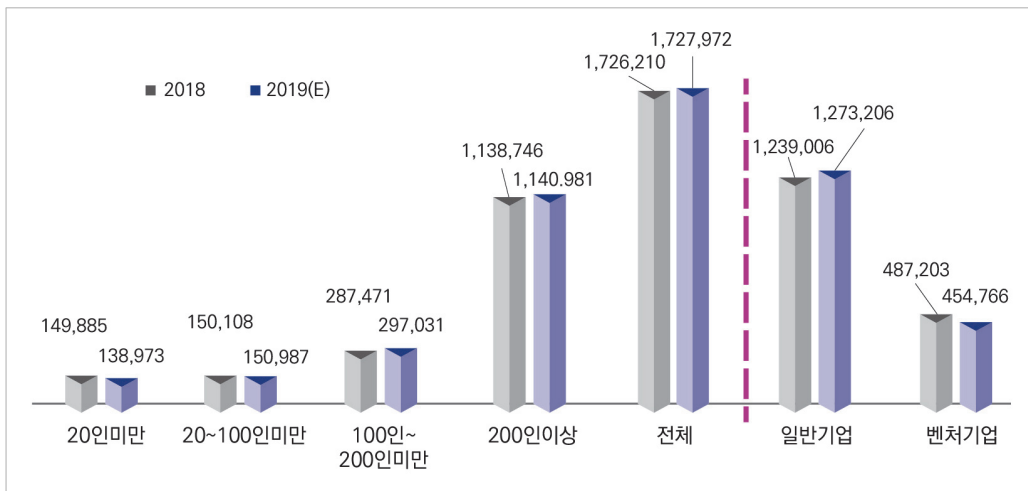
4 서비스별 매출 현황

가. 출동보안서비스

2018년 매출은 1,726,210백만원, 2019년 매출은 1,727,972백만원으로 0.1% 증가한 것으로 조사되었다. 출동보안 서비스는 종사자 수가 100인 미만 기업의 매출액이 297,031백만원, 200인 이상 기업의 매출액이 1,140,981백만원으로 조사되었다. 또한 일반기업의 매출액은 1,273,206백만원으로 벤처기업의 매출액 454,766백만원보다 매우 높은 것으로 나타났다.

[그림 5-11] 출동보안서비스 매출 현황

(단위 : 백만원)

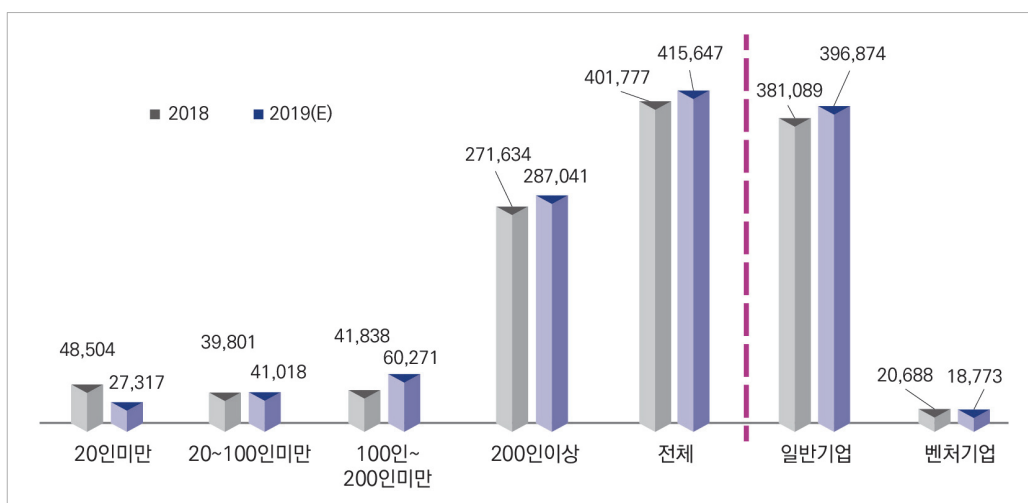


나. 영상보안서비스

2018년 매출은 401,777백만원, 2019년 매출은 415,647백만원으로 3.5% 증가한 것으로 조사되었다. 영상보안 서비스는 100인 이상 200인 미만 기업의 매출액이 60,271백만원이며, 200인 이상 기업의 매출액이 287,041백만원으로 종사자가 200인 이상 기업에서 주로 판매되는 것으로 나타났다. 또한 일반 기업의 매출은 396,874백만원으로 벤처기업 매출 18,773백만원에 비해 매우 높게 나타났다.

[그림 5-12] 영상보안서비스 매출 현황

(단위 : 백만원)

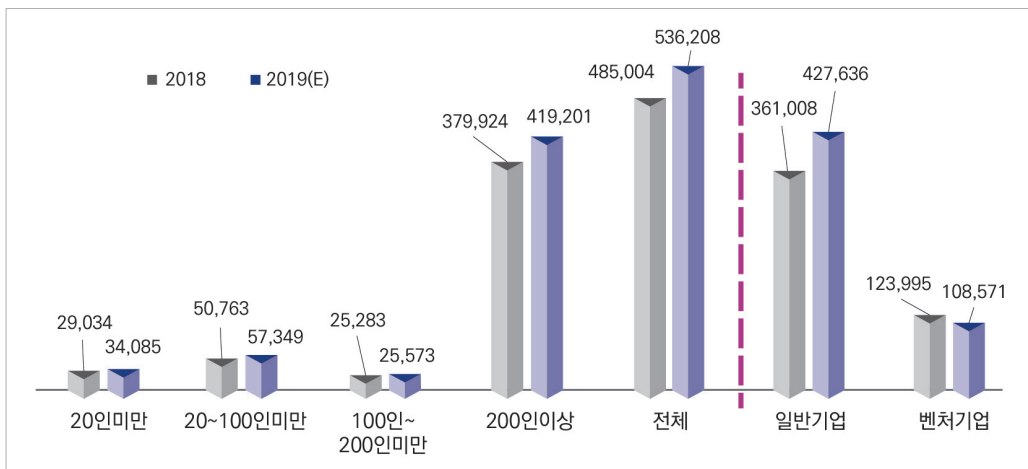


다. 기타보안서비스

2018년 매출은 485,004백만원, 2019년 매출은 536,208백만원으로 10.6% 증가한 것으로 조사되었다. 기타보안 서비스는 20인 이상 100인 미만 기업의 매출액 57,349백만원, 200인 이상 기업의 매출액 419,201백만원으로 종사자가 200인 이상 기업에서 주로 판매되는 것으로 조사되었다. 또한 일반 기업의 매출은 427,636백만원으로 벤처기업 매출 108,571백만원에 비해 매우 높게 나타났다.

[그림 5-13] 기타보안서비스 매출 현황

(단위 : 백만원)



제3절 수출 현황

물리보안산업 수출액은 2018년 1,473,769백만원, 2019년에는 4.3% 증가한 1,537,785백만원이 될 것으로 예상된다. 분야별로 보안용 카메라 제조가 수출 시장에서 차지하는 규모가 2019년 35.2%인 541,936백만원으로 가장 크며, 그 다음으로는 보안용 저장장치 제조가 29.8%인 457,908백만원으로 나타났다.

[표 5-12] 물리보안 제품 수출 현황

(단위 : 백만원, %)

구분		2018년	2019년(E)	증감율(%)	비율(%)
물리보안 시스템 개발 및 공급	보안용 카메라 제조	516,223	541,936	5.0	35.2
	보안용 저장장치 제조	441,229	457,908	3.8	29.8
	CCTV 카메라 부품	174,426	182,749	4.8	11.9
	물리보안 솔루션	106,278	110,988	4.4	7.2
	물리보안 주변장비	23,281	22,424	-3.7	1.5
	출입통제 장비 제조	89,732	96,808	7.9	6.3
	생체인식 보안시스템 제조	22,281	24,203	8.6	1.6
	경보/감시 장비 제조	469	582	24.0	0.04
	기타 제품	99,637	99,864	0.2	6.5
물리보안 관련 서비스	영상보안서비스	33	22	-33.4	0.001
	기타보안서비스	180	301	67.1	0.02
합계		1,473,769	1,537,785	4.3	100.0

수출 대상 지역의 비중을 살펴보면 기타 지역으로의 수출이 43.7%로 가장 높게 나타났다으며, 그 다음으로는 미국이 18.8%인 것으로 조사되었다.

[표 5-13] 물리보안 국가별 수출 현황(2018)

(단위 : %)

구분	수출 국가					
	일본	중국	미국	유럽	기타	합계
비중	12.6	8.6	18.8	16.3	43.7	100.0

1 제품별 수출 현황

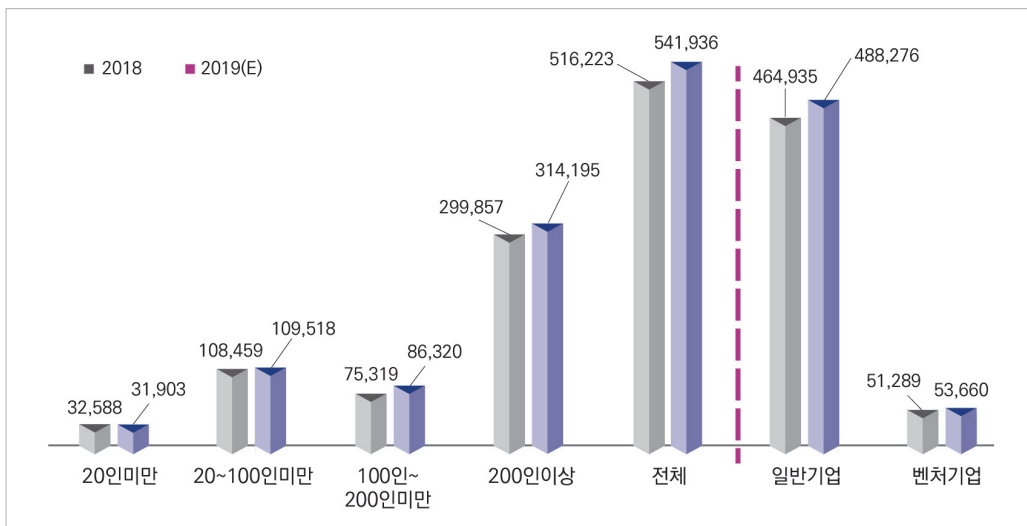
가. 보안용 카메라 제조

보안용 카메라 제조는 네트워크(IP) 카메라, 아날로그 카메라(저해상도), 아날로그 HD카메라(고해상도), 특수카메라(열화상/3D 카메라 등) 제품으로 이들 제품의 2019년 수출액은 541,936백만원으로 2018년 수출액 516,223백만원보다 5.0% 증가한 것으로 조사되었다.

종사자 규모별로 2019년 수출액을 살펴보면 200인 이상 기업들이 314,195백만원을 수출하였으며, 20인 이상 100인 미만 기업들이 109,518백만원을 수출하는 것으로 조사되었다. 기업 형태별로 살펴보면 일반기업이 488,276백만원, 벤처기업은 53,660백만원을 수출하여 일반기업의 수출액이 벤처기업의 수출액보다 매우 높은 것으로 나타났다.

[그림 5-14] 보안용 카메라 제조 제품 수출 현황

(단위 : 백만원)



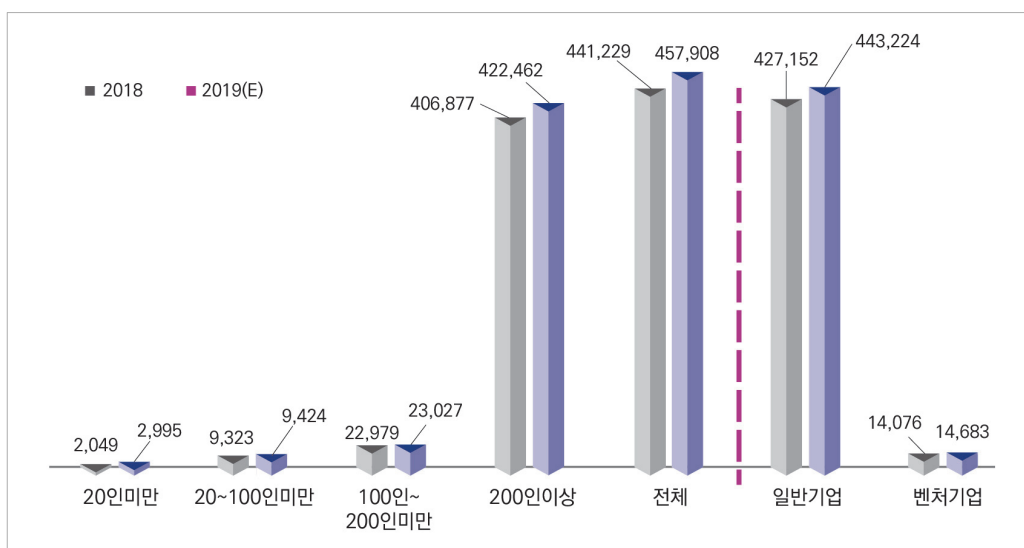
나. 보안용 저장장치 제조

보안용 저장장치 제조는 운영체제 내장 DVR, 운영체제 내장 NVR, PC/서버 기반 DVR, PC/서버 기반 NVR, 예비 저장장치 Backup Storage(콜드스토리지 포함) 등 제품으로 이들 제품의 2019년 수출액은 457,908백만원으로 2018년 수출액 441,229백만원보다 3.8% 증가한 것으로 조사되었다.

종사자 규모별로 2019년 수출액을 살펴보면 200인 이상 기업의 수출액이 422,462백만원으로 대부분을 수출한 것으로 조사되었다. 기업 형태별로 살펴보면 일반기업이 443,224백만원, 벤처기업은 14,683백만원을 수출하여 일반기업의 수출액이 벤처기업의 수출액보다 매우 높은 것으로 나타났다.

[그림 5-15] 보안용 저장장치 제조 수출 현황

(단위 : 백만원)



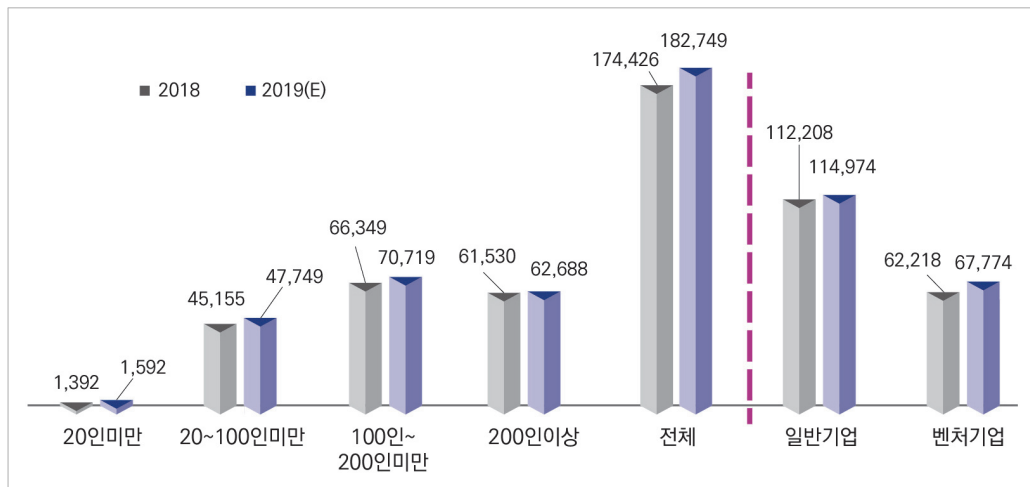
다. CCTV 카메라 부품

CCTV 카메라 부품 제품으로 이들 제품의 2019년 수출액은 182,749백만원으로 2018년 수출액 174,426백만원보다 4.8% 증가한 것으로 조사되었다.

종사자 규모별로 2019년 수출액을 살펴보면 100인 이상 200인 미만 기업들이 70,719백만원을 수출하는 것으로 조사되었으며, 200인 이상 기업들이 62,688백만원을 수출하는 것으로 조사되었다. 기업 형태별로 살펴보면 일반기업이 114,974백만원, 벤처기업은 67,774백만원을 수출하여 일반기업의 수출액이 벤처기업의 수출액보다 높은 것으로 나타났다.

[그림 5-16] CCTV 카메라 부품 수출 현황

(단위: 백만원)



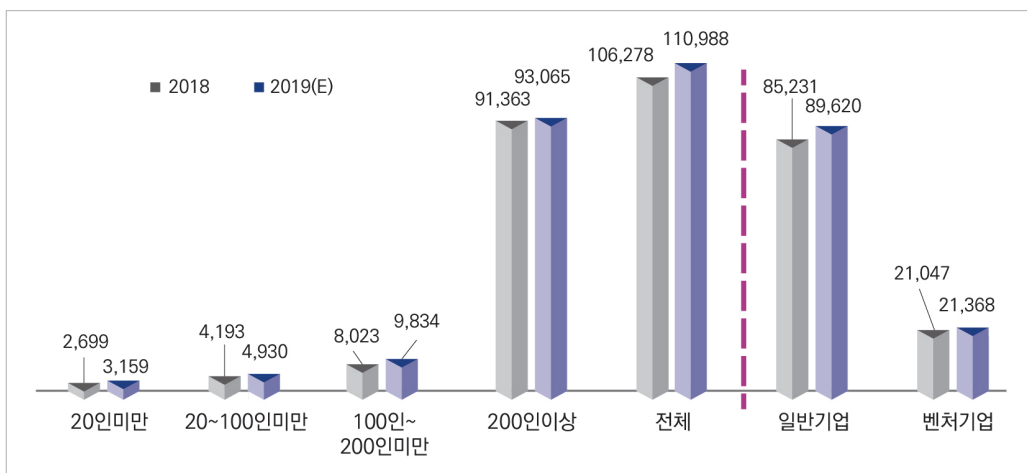
라. 물리보안 솔루션

물리보안 솔루션은 영상감시관제 S/W(CMS/VMS), 지능형 영상감시 솔루션 제품으로 이들 제품의 2019년 수출액은 110,988백만원으로 2018년 수출액 106,278백만원보다 4.4% 증가한 것으로 조사되었다.

종사자 규모별로 2019년 수출액을 살펴보면 200인 이상 기업들이 93,065백만원을 수출하는 것으로 조사되었으며, 100인 이상 200인 미만 기업들이 9,834백만원을 수출하는 것으로 조사되었다. 기업 형태별로 살펴보면 일반기업이 89,620백만원, 벤처기업은 21,368백만원을 수출하여 일반기업의 수출액이 벤처기업의 수출액보다 높은 것으로 나타났다.

[그림 5-17] 물리보안 솔루션 수출 현황

(단위: 백만원)



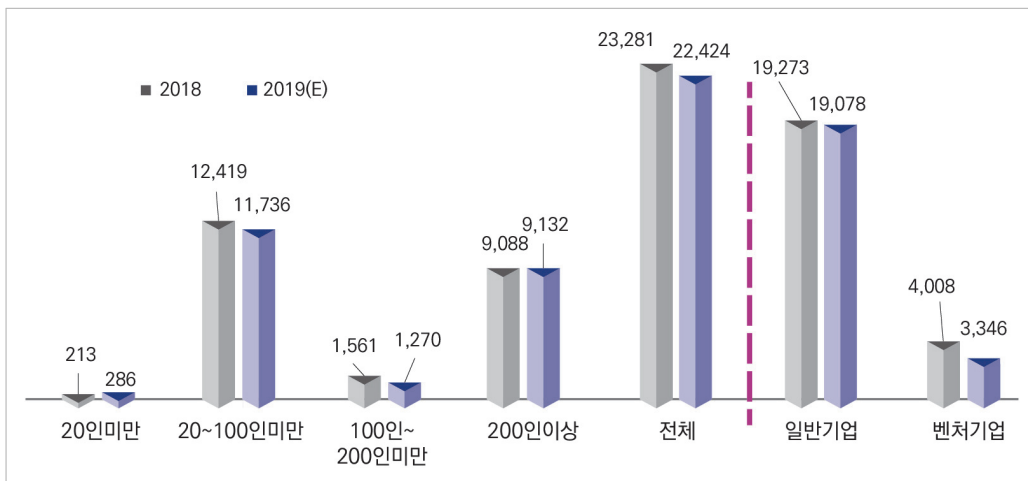
마. 물리보안 주변장비

물리보안 주변장비는 보안통신장비용 모니터, 영상전송/변환장비 및 모듈(비디오서버, 암호화장비, 무선통신용 모듈 등), 전용부품(하우징/브라켓/폴대 등) 제품으로 이들 제품의 2019년 수출액은 22,424백만원으로 2018년 수출액 23,281백만원보다 3.7% 감소한 것으로 조사되었다.

종사자 규모별로 2019년 수출액을 살펴보면 20인 이상 100인 미만 기업들이 11,736백만원을 수출하는 것으로 조사되었으며, 200인 이상 기업들이 9,132백만원을 수출하는 것으로 조사되었다. 기업 형태별로 살펴보면 일반기업이 19,078백만원, 벤처기업은 3,346백만원을 수출하여 일반기업의 수출액이 벤처기업의 수출액보다 높은 것으로 나타났다.

[그림 5-18] 물리보안 주변장비 수출 현황

(단위 : 백만원)



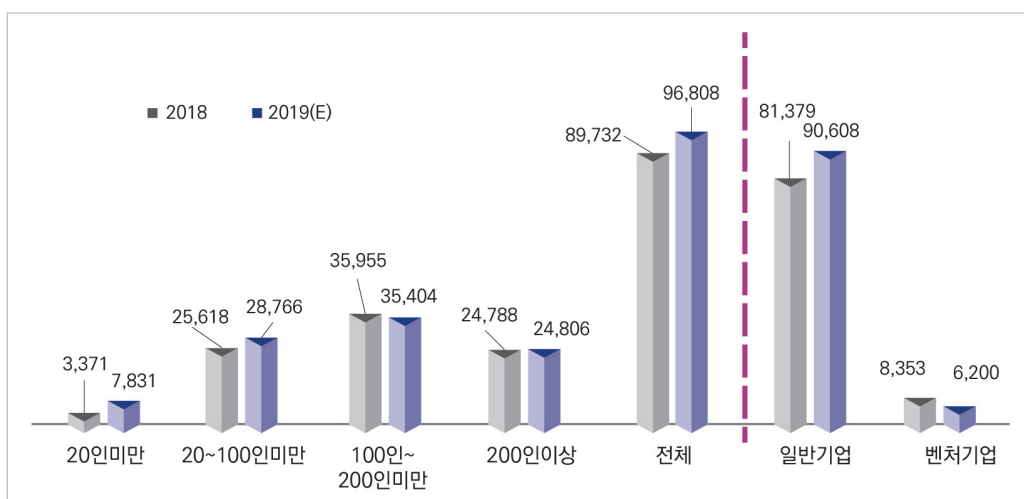
바. 출입통제장비 제조

출입통제장비 제조는 2019년 수출액은 96,808백만원으로 2018년 수출액 89,732백만원보다 7.9% 증가한 것으로 조사되었다.

종사자 규모별로 2019년 수출액을 살펴보면 20인 이상 100인 미만 기업이 28,766백만원, 100인 이상 200인 미만 기업이 35,404백만원을 수출하는 것으로 조사되었다. 기업 형태별로 살펴보면 일반기업의 수출액이 90,608백만원으로 일반기업의 수출액이 대부분을 차지하는 것으로 조사되었다.

[그림 5-19] 출입통제장비 제조 수출 현황

(단위 : 백만원)



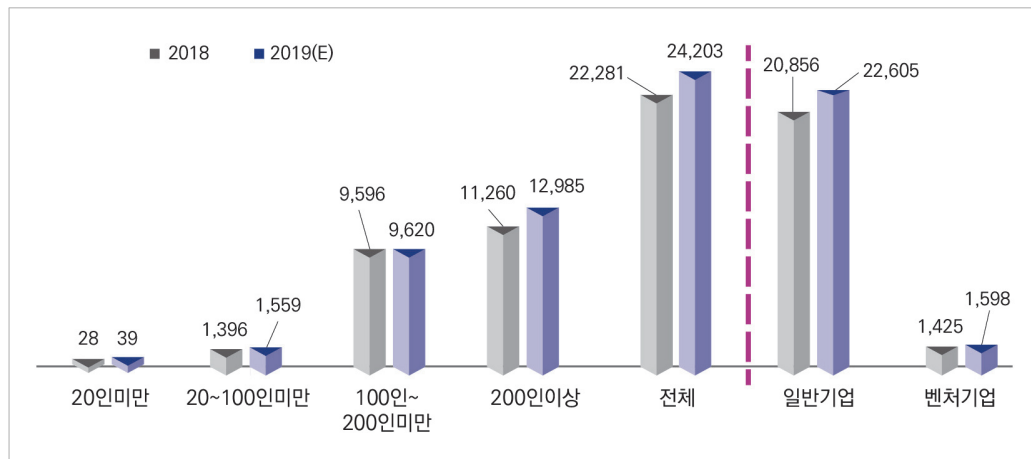
사. 생체인식 보안시스템 제조

생체인식 보안시스템 제조는 기타(음성인식 및 기타), 얼굴인식 시스템, 지문인식 시스템, 홍채인식 시스템 제품으로 이들 제품의 2019년 수출액은 24,203백만원으로 2018년 수출액 22,281백만원보다 8.6% 증가한 것으로 조사되었다.

종사자 규모별로 2019년 수출액을 살펴보면 100인 이상 200인 미만 기업이 9,620백만원을 수출하는 것으로 조사되었으며, 200인 이상 기업이 12,985백만원을 수출하는 것으로 나타났다. 기업 형태별로 살펴보면 일반기업이 22,605백만원, 벤처기업은 1,598백만원을 수출하여 일반기업의 수출이 수출의 대부분을 차지하는 것으로 나타났다.

[그림 5-20] 생체인식 보안시스템 수출 현황

(단위 : 백만원)



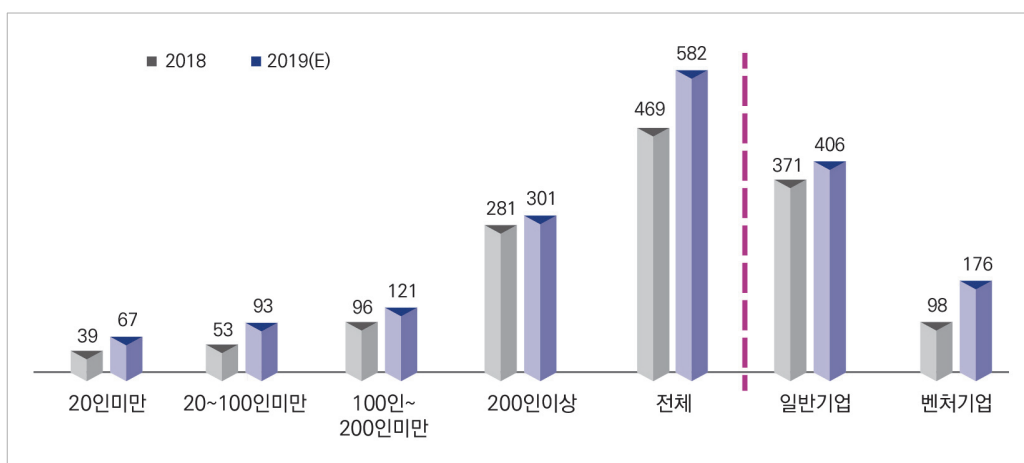
아. 경보/감시 장비 제조

경보/감시 장비 제조의 2019년 수출액은 582백만원으로 2018년 수출액 469백만원보다 24.0% 증가한 것으로 조사되었다.

2019년 수출액을 살펴보면, 종사자 규모별로는 100인 이상 200인 미만 기업이 121백만원을 수출하는 것으로 나타났으며, 200인 이상 기업이 301백만원을 수출하는 것으로 조사되었다. 기업 형태별로는 일반기업이 406백만원, 벤처기업이 176백만원으로 주로 일반기업에서 수출하는 것으로 나타났다.

[그림 5-21] 경보/감시 장비 제품 수출 현황

(단위 : 백만원)



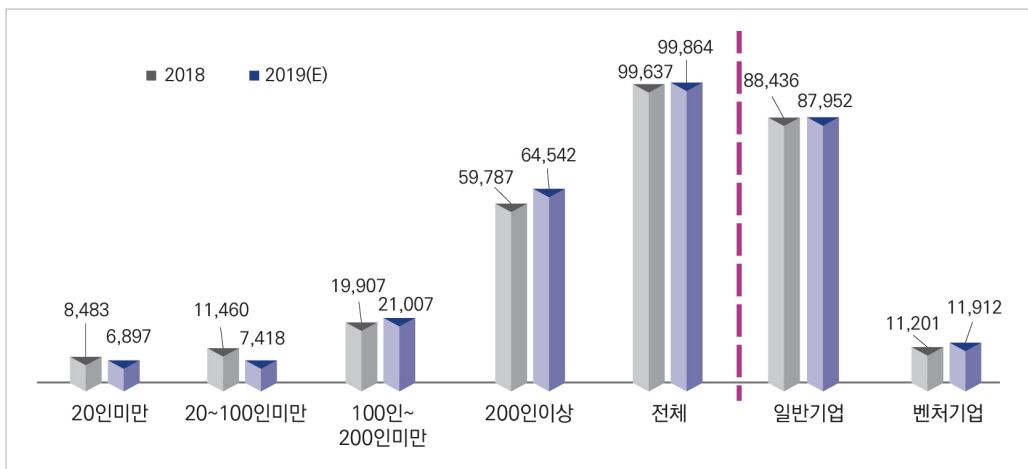
자. 기타 제품

기타 제품의 2019년 수출액은 99,864백만원으로 2018년 수출액 99,637백만원보다 0.2% 증가한 것으로 조사되었다.

2019년 수출액을 살펴보면, 종사자 규모별로는 100인 이상 200인 미만 기업이 21,007백만원을 수출하는 것으로 조사되었으며, 200인 이상 기업은 64,542백만원을 수출하는 것으로 조사되었다. 기업 형태별로 살펴보면 일반기업이 87,952백만원, 벤처기업이 11,912백만원으로 주로 일반기업에서 수출하는 것으로 나타났다.

[그림 5-22] 기타 제품 수출 현황

(단위 : 백만원)



제4절 인력 및 채용 현황

1 인력 현황

물리보안 담당 인원은 32,897명으로 조사되었다. 물리보안 기업 전체 인력 85,361명의 약 38.5% 정도로 파악되었다.

[표 5-14] 물리보안산업 구분별 인력 현황

(2018년 12월 현재)

구분		기업수 (개)	물리보안 담당인력(명)		전체 인력(명)		비중(%)
			합계	평균	합계	평균	
전체		621	32,897	53	85,361	137	38.5
지역	서울	191	15,486	81	39,779	208	38.9
	서울 외	430	17,411	40	45,582	106	38.2
상장 유무	비상장	586	21,999	38	59,400	101	37.0
	코스닥	31	9,872	318	24,361	786	40.5
	유가증권	2	1,013	507	1,567	784	64.6
	코넥스	2	13	7	33	17	39.4
기업 형태	일반기업	344	28,188	82	73,094	212	38.6
	벤처기업	277	4,709	17	12,267	44	38.4
설립 연도	2000년 이전	133	14,217	107	37,031	278	38.4
	2000년 이후- 2005년 이전	153	2,498	16	8,105	53	30.8
	2005년 이후- 2010년 이전	133	10,794	81	26,818	202	40.2
	2010년 이후	202	5,388	27	13,407	66	40.2
종사자	20인 미만	338	1,130	3	3,277	10	34.5
	20인-100인 미만	212	2,897	14	9,177	43	31.6
	100인-200인 미만	33	2,032	62	4,358	132	46.6
	200인 이상	38	26,838	706	68,549	1,804	39.2
자본금	10억 미만	458	3,073	7	11,415	25	26.9
	10억-50억 미만	125	11,927	95	30,930	247	38.6
	50억-100억 미만	28	6,264	224	15,698	561	39.9
	100억 이상	10	11,633	1,163	27,318	2,732	42.6

2 특성별 현황

가. 직종별 인력 현황

특성별 및 직종별로 인력 현황을 살펴보면, 15년 이상은 총 2,594명이었으며 이 중 국내외영업부문이 509명으로 가장 많았고 다음으로 Hardware 부문이 506명, 생산 기술, 품질관리 부문이 456명, 설계, 시공 및 감리 부문이 443명으로 조사되었다.

11년 이상 15년 미만의 경우, Hardware 부문이 1,248명으로 가장 많았고, 다음으로 영업 부문 820명, 생산 기술, 품질 관리 부문이 771명, 응용 Software 부문 643명 순으로 조사되었다. 7년 이상 11년 미만의 경우, 영업 부문이 1,400명으로 가장 많았으며, 4년 이상 7년 미만의 경우, 기타 부문이 2,548명으로 가장 많았으며, 4년 미만의 경우 기타 부문이 3,856명으로 가장 많았다.

[표 5-15] 물리보안산업 특성별 및 직종별 인력 현황

(2018년 12월 현재)

구분	세부 분류	4년 미만	4년 이상 7년 미만	7년 이상 11년 미만	11년 이상 15년 미만	15년 이상	합계(명)	비중(%)
제품 개발	Hardware	1,821	1,478	1,389	1,248	506	6,442	19.6
	응용 Software	1,200	1,279	1,304	643	344	4,770	14.5
영업	국내외 영업	1,108	1,075	1,400	820	509	4,912	14.9
기술 지원	설계, 시공 및 감리	732	1,097	1,064	587	443	3,923	11.9
생산	생산 기술, 품질 관리	1,194	949	1,177	771	456	4,547	13.8
관리 및 기타	관리, 기타	3,856	2,548	1,189	374	336	8,303	25.2
합계		9,911	8,426	7,523	4,443	2,594	32,897	100.0

나. 매출액 규모별 현황

매출액 규모별로 살펴보면, 100억 이상 기업에서 전체 15년 이상 기술자 2,594명 중 2,289명을 보유하고 있으며, 50억 이상 100억 미만 기업이 77명, 10억 이상 50억 미만 기업이 162명, 10억 미만 기업이 66명의 15년 이상 기술자를 보유하고 있는 것으로 조사되었다.

11년 이상 15년 미만 기술자의 경우, 100억 이상 기업이 전체 11년 이상 15년 미만 기술자 4,443명 중 3,920명을 보유하고 있으며, 50억 이상 100억 미만 기업이 104명, 10억 이상 50억 미만 기업체가 301명, 10억 미만 기업이 118명의 11년 이상 15년 미만 기술자를 보유하고 있는 것으로 조사되었다.

7년 이상 11년 미만 기술자는 총 7,523명으로 이 중 6,740명이 100억 이상 기업에서 종사하고 있으며, 50억 이상 100억 미만 기업에 220명, 10억 이상 50억 미만 기업에 426명, 10억 미만 기업에 137명이 종사하고 있는 것으로 조사되었다.

4년 이상 7년 미만 기술자는 총 8,426명으로 이 중 7,664명이 100억 이상 기업에 종사하고 있으며, 217명이 50억 이상 100억 미만 기업에 종사하고, 402명이 10억 이상 50억 미만 기업에 종사하고, 143명이 10억 미만 기업에 종사하고 있는 것으로 조사되었다.

4년 미만 기술자는 총 9,911명으로 이 중 9,234명이 100억 이상 기업에 종사하고 있으며, 168명이 50억 이상 100억 미만 기업에 종사하고, 347명이 10억 이상 50억 미만 기업에 종사하고, 162명이 10억 미만 기업에 종사하고 있는 것으로 조사되었다.

[표 5-16] 물리보안산업 매출액 규모별 인력 현황

(2019년 12월 현재)

매출액 규모	4년 미만	4년 이상 7년 미만	7년 이상 11년 미만	11년 이상 15년 미만	15년 이상	합계(명)
10억 미만	162	143	137	118	66	626
10억~50억 미만	347	402	426	301	162	1,638
50억~100억 미만	168	217	220	104	77	786
100억 이상	9,234	7,664	6,740	3,920	2,289	29,847
합 계	9,911	8,426	7,523	4,443	2,594	32,897

다. 종사자 규모별 현황

종사자 규모별로 살펴보면, 15년 이상 기술자 2,594명 중 200인 이상 기업에 2,010명이 종사하고 있는 것으로 조사되었으며, 100인 이상 200인 미만 기업에 207명, 20인 이상 100인 미만 기업에 269명, 20인 미만 기업에 108명이 종사하고 있는 것으로 조사되었다.

11년 이상 15년 미만의 경우, 총 4,443명 중 200인 이상 기업에 3,426명이 종사하고 있으며, 100인 이상 200인 미만 기업에 316명, 20인 이상 100인 미만 기업체에 520명, 20인 미만 기업체에 181명이 종사하고 있는 것으로 조사되었다.

7년 이상 11년 미만의 경우, 총 7,523명 중 200인 이상 기업체에 5,776명이 종사하고 있으며, 100인 이상 200인 미만 기업에 633명, 20인 이상 100인 미만 기업체에 856명, 20인 미만 기업체에 258명이 종사하고 있는 것으로 조사되었다.

4년 이상 7년 미만의 경우, 총 8,426명 중 6,980명이 200인 이상 기업체에 종사하고 있으며, 100인 이상 200인 미만 기업체에 489명, 20인 이상 100인 미만 기업체에 680명, 20인 미만 기업체에 277명이 종사하고 있는 것으로 조사되었다.

4년 미만의 경우, 총 9,911명 중 8,646명이 200인 이상 기업체에 종사하고 있으며, 100인 이상 200인 미만 기업체에 387명, 20인 이상 100인 미만 기업체에 572명, 20인 미만 기업체에 306명이 종사하고 있는 것으로 조사되었다.

[표 5-17] 물리보안산업 종사자 규모별 인력 현황

(2018년 12월 현재)

종사자 규모	4년 미만	4년 이상 7년 미만	7년 이상 11년 미만	11년 이상 15년 미만	15년 이상	합계(명)
20인 미만	306	277	258	181	108	1,130
20인-100인 미만	572	680	856	520	269	2,897
100인-200인 미만	387	489	633	316	207	2,032
200인 이상	8,646	6,980	5,776	3,426	2,010	26,838
합 계	9,911	8,426	7,523	4,443	2,594	32,897

라. 기업 형태별 현황

물리보안 기업의 경우 기업 형태별 기술 등급별 종사자 수를 살펴보면 15년 이상 기술자는 2,594명 중 일반기업에 2,215명, 벤처기업에 379명이 종사하고 있는 것으로 조사되었으며, 11년 이상 15년 미만 기술자의 경우, 4,443명 중 일반기업에 3,728명, 벤처기업에 715명이 종사하고 있는 것으로 조사되었다. 7년 이상 11년 미만 기술자의 경우 7,523명 중 일반기업에 6,477명, 벤처기업에 1,046명이 종사하는 것으로 조사되었으며, 4년 이상 7년 미만 기술자의 경우 8,426명 중 일반기업에 7,199명, 벤처기업에 1,227명이 종사하고 있는 것으로 조사되었으며, 4년 미만 기술자의 경우 9,911명 중 일반기업에 8,569명, 벤처기업에 1,342명이 종사하고 있는 것으로 조사되었다.

[표 5-18] 물리보안산업 기업 형태별 인력 현황

(2018년 12월 현재)

기업 형태	4년 미만	4년 이상 7년 미만	7년 이상 11년 미만	11년 이상 15년 미만	15년 이상	합계(명)
일반기업	8,569	7,199	6,477	3,728	2,215	28,188
벤처기업	1,342	1,227	1,046	715	379	4,709
합 계	9,911	8,426	7,523	4,443	2,594	32,897

3 채용 현황

가. 분야별 채용 현황

2019년도 물리보안 기업의 분야별 인력 채용 계획을 살펴보면, 2,852명의 인력 채용을 할 것으로 조사되었으며 1,686명이 경력직으로 채용할 것으로 조사되었다.

[표 5-19] 물리보안산업 인력 채용 현황

(2019년 예상)

구분	2019년(채용)
신입	1,166
경력	1,686
합계(명)	2,852

나. 매출액 규모별 채용 현황

매출액 규모별로 인력채용 계획을 살펴보면 100억 이상 기업이 2,852명 중 2,424명을 채용할 예정이었으며, 10억 이상 50억 미만 기업의 경우 274명, 50억 이상 100억 미만 기업이 106명을 채용할 것으로 조사되었다.

매출액 규모별로 살펴보면, 기업 규모에 관계없이 신입직보다는 경력직을 더 많이 채용할 것으로 조사되었다.

[표 5-20] 물리보안 매출액 규모별 인력 채용 현황

(2019년 예상)

매출액 규모	2019년(채용)		합계(명)
	신입	경력	
10억 미만	20	28	48
10억-50억 미만	137	137	274
50억-100억 미만	38	68	106
100억 이상	971	1,453	2,424
합계	1,166	1,686	2,852

다. 종사자 규모별 채용 현황

종사자 규모별 인력 채용 계획을 살펴보면 20인 미만 기업체에서 105명을 채용할 예정이며, 20인 이상 100인 미만 기업이 330명, 100인 이상 200인 미만 기업이 244명, 200인 이상 기업이 2,173명을 채용할 것으로 조사되었다.

[표 5-21] 물리보안 종사자 규모별 인력 채용 현황

(2019년 예상)

종사자 규모	2019년(채용)		합계(명)
	신입	경력	
20인 미만	48	57	105
20인-100인 미만	140	190	330
100인-200인 미만	82	162	244
200인 이상	896	1,277	2,173
합계	1,166	1,686	2,852

라. 기업 형태별 채용 현황

기업 형태별 인력 채용 계획을 살펴보면, 총 2,852명 중 일반기업이 2,258명, 벤처기업이 594명을 채용할 것으로 조사되었다.

[표 5-22] 기업 형태별 인력 채용 현황

(2019년 예상)

기업 형태	제품개발(명)		합계(명)
	신입	경력	
일반기업	922	1,336	2,258
벤처기업	244	350	594
합계	1,166	1,686	2,852

4 채용 계획

물리보안관련 기업체의 2020년 신규 예정 채용인력은 총 2,787명으로 조사 되었다. 신입직보다는 경력직의 채용 비중이 높게 나타났다.

[표 5-23] 물리보안산업 분야별 채용 계획

(2020년 예상)

	채용계획(명)
신입	1,131
경력	1,656
합계(명)	2,787

채용 예정 인원은 매출액 규모가 100억 이상 기업에서 2,551명을 채용 예정인 것으로 조사되었으며, 종사자 규모별로는 100인 이상 기업에서 2,317명을 채용할 예정인 것으로 조사되었다. 기업형태별로 살펴보면, 일반기업이 2,253명을 채용할 예정이며 벤처기업이 534명을 채용할 예정인 것으로 조사되었다.

[표 5-24] 물리보안 기업 특성별 채용 계획

(2020년 예상)

구분		계획인원(명)	
		신입	경력
매출액 규모	10억 미만	18	17
	10억~50억 미만	77	80
	50억~100억 미만	20	24
	100억 이상	1,016	1,535
종사자 규모	10인 미만	30	33
	10인~50인 미만	77	104
	50인~100인 미만	93	133
	100인 이상	931	1,386
기업형태	일반기업	892	1,361
	벤처기업	239	295

제5절 기술개발 및 동향

1 자체기술연구소 및 연구개발 전담부서 운영

물리보안기업의 기술개발 관련 자체기술연구소 및 전담부서 운영 현황을 조사한 결과, 기업부설연구소를 운영하는 기업은 359개 57.8%, 연구개발전담부서를 운영하는 기업은 148개 23.8%로 조사되었다. 반면 기업부설연구소와 연구개발 전담부서를 하나도 운영하지 않는다는 기업은 114개 18.4%로 나타났다.

[표 5-25] 물리보안 자체기술연구소 및 전담부서 운영 현황

(단위 : 개, %)

구분	종사자 기준				운영현황	
	20인 미만	100인 미만	200인 미만	200인 이상	합계	비율(%)
기업부설연구소 운영	155	156	23	25	359	57.8
연구개발전담부서 운영	94	41	10	3	148	23.8
없음	89	15	0	10	114	18.4
합계	338	212	33	38	621	100.0

2 연도별 기술개발 투자액 현황

물리보안 기업의 연도별 기술개발 투자액 현황 및 향후 전망을 조사한 결과, 2018년도 전체 투자 기업은 모두 218개이며, 기업당 평균 951.4백만원, 연구개발 투자 기업은 217개로 기업 평균 643.2백만원을 투자한 것으로 나타났다.

2019년도 전체 투자 기업은 210개 평균 482.6백만원, 연구개발 투자 기업은 205개 기업 평균 468.7백만원을 투자한 것으로 나타났다.

향후 2020년 기술연구 전체 투자 기업은 210개 기업 평균 489.1백만원, 연구개발 투자 기업은 205개 기업 평균 454.8백만원을 투자할 것으로 조사되었다.

매출액 대비 기술개발 투자비율은 2018년도에는 9.4%, 2019년도에는 8.5%, 2020년도에는 9.0%로 나타났다.

[표 5-26] 물리보안 기업 연도별 기술개발 투자액 현황

(단위 : 개, 백만원, %)

구분	2018년		2019년(E)		2020년(E)	
	기업수	투자액 평균	기업수	투자액 평균	기업수	투자액 평균
전체 투자액 (연구개발/건물/기계/설비 등)	218	951.4	210	482.6	210	489.1
연구개발 투자액	217	643.2	205	468.7	205	454.8
매출 대비 투자 비율(%)	9.4		8.5		9.0	

3 기술개발시 애로사항

물리보안 기업들은 기술개발 시 애로사항으로 자금조달이 34.1%로 가장 높은 것으로 조사되었다. 다음으로 기술개발 인력확보 및 유지가 30.4%, 그 다음으로는 기술정보 부족 및 획득 곤란이 15.6%, 연구 설비 기자재 부족이 9.6%, 기타 5.9%로 조사되었다.

[표 5-27] 물리보안 기술개발시 애로사항(복수응답)

구분	비율(%)
기술개발 인력 확보 및 유지	30.4
자금조달	34.1
연구 설비 기자재 부족	9.6
신기술의 짧은 수명주기	4.4
기술정보 부족 및 획득 곤란	15.6
기타	5.9
합계	100

4 지식재산권 보유 현황

물리보안 관련 지식재산권 보유현황을 조사한 결과, 현재 보유하고 있거나 출원 중인 지식재산권은 5,317건으로 나타났다. 이를 구체적으로 살펴보면 현재 보유 중인 지식재산권이 4,973건이며, 출원 중인 지식재산권이 344건인 것으로 조사되었다.

현재 보유 중인 물리보안 지식재산권을 보면 특허권 4,347건 87.4%, 실용신안권 99건 2.0%, 의장권 69건 1.4%, 상표권 458건 9.2%로 조사되었다.

현재 출원 중인 지식재산권을 구체적으로 살펴보면 특허권 314건 91.3%, 실용신안권 8건 2.3%, 상표권 22건 6.4%로 조사되었다.

한편, 해외 특허의 경우 기업 당 평균 2.3건을 보유하고 있으며, 기업당 평균 2.0건을 출원 중에 있는 것으로 조사되었다.

[표 5-28] 물리보안 지식재산권 보유 현황

구분		현재 보유		현재 출원 중	
		건수(건)	비율(%)	건수(건)	비율(%)
지식재산권	특허권	4,347	87.4	314	91.3
	실용신안권	99	2.0	8	2.3
	의장권	69	1.4	0	0.0
	상표권	458	9.2	22	6.4
합계		4,973	100.0	344	100.0

[표 5-29] 물리보안 해외특허 보유 현황

(단위 : 개, %, 건)

건수	보유기업 수	보유기업 비율(%)	총 건수	평균 건수
현재 보유	171	27.5	389	2.3
현재 출원 중	153	24.6	301	2.0

5 매출 규모별 제품비중

매출 규모별 제품비중을 조사한 결과, 자사제품 판매 비율이 77.2%, 국내 타사 제품 유통비율이 18.5%, 외산제품 유통이 4.3%로 조사되었다.

[표 5-30] 물리보안 매출규모별 제품비중

(단위 : %)

구분	비중
자사제품 판매	77.2
국내 타사제품 유통	18.5
외산제품 유통	4.3
합계	100.0

6 주요 경쟁 요소

물리보안 기업의 주요 경쟁 요소를 살펴보면 기술, 품질 요소가 주요 경쟁 요소라고 응답한 비율이 매우 높게 나타나는 것으로 조사되었다.

기술/품질, 가격, 인지도, 마케팅, 입지적 유리, 기타 6개 항목에 대해 주요 경쟁 요소를 조사한 결과 기술, 품질이 주요 경쟁 요소라고 응답한 비율이 42.4%로 가장 높은 것으로 나타났다. 그 다음으로는 가격이 27.3%, 마케팅 16.3%로 나타났으며, 인지도는 11.4%, 입지적 유리 1.8%로 조사되었다.

[표 5-31] 물리보안 주요 경쟁 요소(복수응답)

구분	빈도(개)	비율(%)
기술, 품질	213	42.4
가격	137	27.3
마케팅	82	16.3
인지도	57	11.4
입지적 유리	9	1.8
기타	4	0.8
합계	502	100.0

7 상장 유무별 현황

물리보안 기업들은 경영/기술 정보를 주로 동종업체간 교류, 박람회/전시회, 관련 업종단체/협회 등으로부터 수집하는 것으로 조사되었다. 제품/서비스 협력업체로부터 정보를 수집한다는 응답이 40.1%로 가장 높은 비중을 차지하는 것으로 조사되었다. 다음으로 고객(납품 모기업)이 16.7%로 높게 나타났으며, 그 다음으로 정부 및 공공기관, 관련 업종단체/협회가 각각 14.6%, 11.7%로 조사되었다. 이외에도 대학/연구소, 금융기관이 각각 8.2%, 4.0% 등으로 조사되었다.

[표 5-32] 물리보안 경영/기술정보 수집 경로(복수응답)

구분	빈도(개)	비율(%)
대학/연구소	31	8.2
정부 및 공공기관	55	14.6
고객(납품 모기업)	63	16.7
제품/서비스 협력업체	151	40.1
관련 업종단체/협회	44	11.7
컨설팅업체	3	0.8
금융기관	15	4.0
동종업체간 교류	9	2.4
기타	6	1.6
합계	377	100.0

8 시장 경쟁 및 산업 동향 등의 수준

물리보안 시장에 대한 성장성의 경우 신기술, 신제품의 지속적 출현과 기술 변화의 예측에 대해서는 긍정적으로 평가하나, 기업 이윤의 안정적 확보에 대해서는 동의 정도가 낮은 것으로 조사되었다. 경쟁성의 경우 가격 경쟁, 외산과의 경쟁이 매우 치열하다고 평가하는 것으로 조사되었다. 또한 기타 구분으로 자금상황이 어려운 편이라고 응답하는 기업이 많은 것으로 조사되었다.

[표 5-33] 물리보안 시장 경쟁 및 산업 동향 등의 수준

(단위 : 점, 5점 만점)

구분	시장 상황 및 산업 동향	동의 수준
성장성	신기술, 신제품이 지속적으로 출현하고 있다.	3.43
	기업 이윤을 안정적으로 확보할 수 있다.	3.12
	기술 변화의 예측이 어느 정도 가능하다.	3.41
경쟁성	시장 규모가 포화상태이다	3.67
	가격 경쟁이 치열하다.	4.28
	경쟁자 전략의 예측이 가능하다.	3.51
	신기술 습득을 위한 경쟁이 치열하다.	3.89
	국산과 외산의 경쟁이 증가하고 있다.	3.80
기술력	국내시장 기술력이 낮다.	2.73
	통합솔루션 제공이 미약하다.	3.24
기타	자금상황이 어려운 편이다.	3.57

9 시장 확대를 위한 정부지원 필요 부분

시장 확대를 위한 정부 지원에 대해 물리보안 기업들은 기술개발 지원, 자금지원 및 세제혜택에 대한 요구 수준이 높은 것으로 조사되었다.

[표 5-34] 물리보안 시장 확대를 위한 정부 지원 필요 사항(복수응답)

구 분	빈도(개)	비율(%)
전문인력 양성	15	7.1
기술개발 지원	59	28.0
기술이전의 활성화	13	6.2
법/제도 제 개정	25	11.8
공공부문의 시장수요 창출	20	9.5
소비촉진/투자활성화	14	6.6
자금지원 및 세제혜택	58	27.5
해외지원 사업 확대	5	2.4
기타	2	0.9
합계	211	100.0

10 해외 진출시 애로사항

물리보안 기업들의 해외 진출 시 애로사항으로 판로개척이 3.91점으로 가장 높게 나타나며, 해외진출 위한 관련 정보 3.74점, 자금유동성 부족 3.64점, 세계경제 불안 및 경기둔화 3.55점, 환율하락에 따른 채산성 악화 3.54점, 인력 부족 3.52점, 국제표준 및 인증획득 3.49점 등이 상대적으로 높게 조사되었다.

[표 5-35] 물리보안산업 해외 진출시 애로사항

(단위 : 점, 5점 만점)

애로사항	수준
환율하락에 따른 채산성 악화	3.54
자금유동성 부족	3.64
현지 법 및 제도	3.46
판로개척	3.91
관세·통관절차 부담	3.52
지적재산권 보호역량 부족	3.39
국제표준 및 인증획득	3.49
해외진출 위한 관련 정보	3.74
세계경제 불안 및 경기둔화	3.55
인력 부족	3.52

2019

국내 정보보호산업
실태조사



제6장

정책적 시사점

1	정보보호 기업체 수의 증가	137
2	정보보호산업의 성장세 지속	138
3	정보보안 분야의 서비스 시장 성장 강세	139
4	정보보안산업의 수출 규모 크게 성장	140
5	정보보호 기업의 일자리 창출	141

6장

정책적 시사점

1 정보보호 기업체 수의 증가

정보보호산업에서 비즈니스 활동을 하는 참여기업 수가 2018년도 1013개에서 2019년도에는 1,094개로 8.0% 증가한 것으로 나타났다. 특히, 물리보안 기업은 549개에서 621개로 증가하였는데, 이는 물리보안분야에서 비즈니스 기회가 많아지고 있기 때문에 기업들의 참여가 높아지고 있다는 것을 의미하고, 그 규모도 커지고 있다는 것으로 해석할 수 있다. 정보보호 기업체 수의 증가는 정보보호시장이 꾸준히 성장하고 있다는 것을 의미한다.

[표 6-1] 정보보호 기업 종사자 규모 변화

(단위 : 개)

구분	정보보안		물리보안		합계	
	기업수 (2018)	기업수 (2019)	기업수 (2018)	기업수 (2019)	기업수 (2018)	기업수 (2019)
20인 미만	226	181	340	338	566	519
20인~100인 미만	161	200	129	212	290	412
100인~200인 미만	43	52	49	33	92	85
200인 이상	34	40	31	38	65	78
합계	464	473	549	621	1,013	1,094

2 정보보호산업의 성장세 지속

정보보호산업의 성장률은 2017년에는 6.0%, 2018년에는 5.6%에서 2019년에는 4.3% 성장하는 등 매년 성장세가 꾸준히 지속되고 있는 것으로 나타났다. 2018년도에는 정보보호시장 규모는 10조원을 돌파한 것으로 추정되고, 정보보안시장 규모도 3조 원 돌파, 규모도 7조원을 돌파한 것으로 추정된다. 다만, 정보보호시장규모 성장률의 증가폭은 다소 완화되어 향후에도 성장폭은 점점 낮아질 것으로 보인다.

[표 6-2] 정보보호산업 매출과 성장률 추이

(단위: 백만원, %)

구분	정보보안		물리보안		합계	
	매출액	성장률	매출액	성장률	매출액	성장률
2016	2,454,024	16.4	6,588,787	7.8	9,042,811	10.0
2017	2,744,940	11.9	6,840,822	3.8	9,585,762	6.0
2018	3,082,926	12.3	7,034,918	2.8	10,117,844	5.6
2019e	3,277,687	6.3	7,279,550	3.5	10,557,237	4.3

정보보안은 2018년에는 12.3%, 2019년도에는 6.3% 성장한 것에 비해, 물리보안은 2018년에는 2.8%, 2019년도에는 3.5% 성장한 것으로 나타났다. 2013년 이전에는 정보보안시장에 비해 물리보안시장의 성장률이 더 높았으나 2014년 이후에 물리보안 시장의 성장률은 정보보안에 비해 다소 주춤한 것으로 보인다. 정보보안 시장이 지속적으로 성장하고 있는 것은 사이버보안 관련 정부의 법·제도의 정비, 정보보호산업의 진흥에 관한 법률 정비, 여러 차례의 사이버 보안사고로 인한 경각심 고조, 정부 및 기업의 보안 투자 강화, 해외 진출 노력 등이 시장에 반영된 것으로 보인다.

3 정보보안 분야의 서비스 시장 성장 강세

2019년도 정보보안 분야의 성장은 정보보안시스템 개발 및 공급시장이 7.0%, 정보보안 관련 서비스 시장은 4.8% 증가한 것으로 나타나 전체 규모와 최근 성장추세를 정보보안시스템 개발 및 공급시장이 주도하고 있는 것으로 나타났다.

[표 6-3] 정보보안산업 중분류 매출 증감 현황

(단위 : 백만원, %)

구분		2018년	2019년	증감율(%)
정보보안 시스템 개발 및 공급	네트워크보안 시스템 개발	729,393	771,656	5.8
	시스템보안 솔루션 개발	488,402	523,115	7.1
	정보유출방지 시스템 개발	426,128	456,251	7.1
	암호/인증 시스템 개발	151,879	161,760	6.5
	보안관리 시스템 개발	297,920	327,790	10.0
	소계	2,093,723	2,240,572	7.0
정보 보안 관련 서비스	보안컨설팅 서비스	302,099	321,478	6.4
	보안 시스템 유지관리/ 보안성지속 서비스	351,942	359,645	2.2
	보안관제 서비스	273,927	286,880	4.7
	보안교육 및 훈련 서비스	1,740	2,990	71.8
	공인/사설 인증서	59,496	66,122	11.1
	소계	989,203	1,037,115	4.8
전체		3,082,926	3,277,687	6.3

정보보안시스템 개발 및 공급시장은 암호/인증 시스템 개발분야의 성장이 상대적으로 가장 낮고, 다른 분야는 대체로 비슷한 것으로 나타났다. 정보보안서비스 중에서 보안교육 및 훈련 서비스 분야에서는 가장 크게 성장하였는데 이는 기업들이 스스로 정보보호 수준제고를 위해 ISMS, PIMS 등의 인증심사를 받고자 정보보호컨설팅을 적극 활용하고 있는 것으로 파악된다. 향후에도 ISMS 의무화 대상자 확대 등에 따라 보안교육 및 훈련 서비스, 보안컨설팅 시장은 지속적으로 성장할 것으로 예상된다.

4 정보보안산업의 수출 규모 크게 성장

정보보호산업의 수출은 2017년의 경우 2016년 대비 1.1% 감소하였고, 2018년에는 전년 대비 -0.9% 감소, 2019년에는 전년 대비 5.8% 증가한 것으로 나타났다. 최근 이러한 증가 추세에도 불구하고 수출액은 2015년 1,623,673백만원 수준을 회복하는 정도에 그친 것으로 나타나 지속적인 수출 경쟁력 확보가 필요하다고 판단된다.

[표 6-4] 정보보호산업 연평균 수출 성장률

(단위: 백만원, %)

구분	정보보안		물리보안		합계	
	수출액	증가율	수출액	증가율	수출액	증가율
2016	88,978	13.9	1,400,102	-9.4	1,489,080	-8.3
2017	94,398	6.1	1,475,755	5.4	1,570,153	-1.1
2018	82,363	-12.7	1,473,769	-0.1	1,556,132	-0.9
2019e	108,528	31.8	1,537,785	4.3	1,646,313	5.8

전체적인 규모면에서는 물리보안 분야의 수출액이 훨씬 크나, 최근 정보보안분야 수출 증가율은 물리보안분야 보다 높아 정보보안 분야의 해외 경쟁력이 점차 나아지고 있는 것으로 추정된다. 특히, 2019년에는 정보보안분야의 수출증가율이 역대 최고치로 증가한 것을 볼 때, 앞으로도 해외시장 진출을 통한 정보보안산업의 경쟁력이 높아질 것으로 기대된다.

정보보안 기업과 물리보안 기업들이 해외 진출시 가장 큰 애로사항으로는 판로개척이 공통적으로 높게 파악되고 현지 법·제도에 대한 이해부족이 높은 것으로 파악된다. 따라서 정보보호산업의 국제경쟁력 제고를 위해서는 정부차원에서 다양한 전시회 등을 통해 판로개척 활동을 지원해 주고, 해외에 상주하는 공공기관 등을 통해 해외 현지 법·제도에 대한 가이드북 제작·배포를 통해 정보를 제공하는 것이 필요하다고 판단된다.

5 정보보호 기업의 일자리 창출

정보보호 기업에 종사하는 인력은 2018년 44,029명에서 2019년 46,275명으로 전년 대비 5.1% 증가한 것으로 나타났다. 특히 정보보안 기업에 종사하는 인력이 10.9% 증가한 것에 비해, 물리보안 기업에 종사하는 인력은 2.9% 증가한 것에 그친 것으로 나타나, 정보보안 기업은 시장규모에 비해 상대적으로 더 많은 일자리 증가에 기여하고 있는 것으로 추정된다.

[표 6-5] 정보보호기업 인력현황

(단위: 명)

구분	정보보안	물리보안	합계
2018년 (2017년 12월)	12,068	31,961	44,029
2019년 (2018년 12월)	13,378	32,897	46,275

'19년도 정보보호기업의 신규 채용자(계획포함)는 4,658명이며, '20년도에는 4,121명 정도를 추가로 채용할 계획인 것으로 나타났다. 다만, 분야별 '19년 신규 채용인원(계획포함)은 정보보안 1,806명, 물리보안은 2,852명이고, '20년 신규 채용계획은 정보보안 1,334명, 물리보안은 2,787명으로 20년도에는 일자리 창출측면에서 물리보안 분야의 기여도가 높을 것으로 추정된다.

[표 6-6] '19년 신규채용 현황 및 '20년 계획

(단위: 명, %)

구분	2019			2020(E)		
	정보보안	물리보안	합계	정보보안	물리보안	합계
인원수	1,806	2,852	4,658	1,334	2,787	4,121
비중	38.8	61.2	100	32.4	67.6	100

참 고 문 헌

1 국문

- 국가정보원·방송통신위원회. 2016 국가정보보호백서. 2016.
- 한국정보화진흥원. 2014 국가정보보호백서. 2014.
- 국가정보원·방송통신위원회. 2010 국가정보보호백서. 2010.
- 국가정보원·방송통신위원회. 2009 국가정보보호백서. 2009.
- 국가정보원·방송통신위원회. 2008 국가정보보호백서. 2008.
- 국가정보원·정보통신부. 2007 국가정보보호백서. 2007.
- 국가정보원·정보통신부. 민간부문 정보보호 정책 연혁. 2004.
- 정보통신부. 정보보호산업 발전대책(1998-2002). 1997.
- 정보통신부. 정보화역기능 방지 종합대책(안). 1999.
- 정보통신부. 유비쿼터스 정보보호 기본전략. 2006.
- 정보통신부·한국정보보호진흥원. 민간부문 정보보호 정책 연혁. 2004.
- 지식경제부. 정보보호산업 발전전략. 2008.
- 한국전자통신연구원. 정보보호 기술 및 제품 경쟁력 분석서. 2006.
- 한국정보보호연합회. 정보산업 민간백서. 제19집. 2008.
- 한국정보보호진흥원. “국내외 정보보호산업 현황 및 주요 정책 진단: FTA 등 시장개방
화 환경을 중심으로.” 정보보호 Issue Report 2007-06. 2007a.
- 한국정보보호산업협회. 2017 국내 정보보호산업 실태조사. 2017.
- 한국정보보호산업협회. 2016 국내 정보보호산업 실태조사. 2016.
- 한국인터넷진흥원. 2015 국내 정보보호산업 실태조사. 2015.
- 한국인터넷진흥원. 2014 국내 정보보호산업 실태조사. 2014.
- 한국인터넷진흥원. 2013 국내 정보보호산업 실태조사. 2013.
- 한국인터넷진흥원. 2012 국내 지식정보보안산업 실태조사. 2012.
- 한국인터넷진흥원. 2011 국내 정보보안산업 실태조사. 2011.
- 한국인터넷진흥원. 2010 국내 정보보안산업 실태조사. 2010.
- 한국인터넷진흥원. 2009 국내 정보보호산업 시장 및 동향 조사. 2009.

한국인터넷진흥원. 2008 국내 정보보호산업 시장 및 동향 조사. 2008.

한국인터넷진흥원. 2007 국내 정보보호산업 시장 및 동향 조사. 2007.

한국인터넷진흥원. 2006 국내 정보보호산업 통계조사. 2006.

한국인터넷진흥원. 2005 국내 정보보호산업 통계조사. 2005.

한국인터넷진흥원. 2004 국내 정보보호산업 통계조사. 2004.

한국인터넷진흥원. 2003 국내 정보보호산업 통계조사. 2003.

한국인터넷진흥원. 2002 국내 정보보호산업 통계조사. 2002.

한국인터넷진흥원. 2001 국내 정보보호산업 실태조사. 2001.

한국인터넷진흥원. 2009년 정보보호 실태조사. 2009.

한국인터넷진흥원. 2008년 정보보호 실태조사. 2008.

한국인터넷진흥원. 2007년 정보보호 실태조사. 2007.

한국정보통신기술협회. 정보보호전문용어사전. 2006.

IDC. 세계 정보보호산업 시장 전망 보고. 2008.

김정덕 외 2명, “융합보안의 개념 정립과 접근방법”, 정보보안학회지, 2009.12

이동휘 외 1명, “융합보안관제시스템 개선에 관한 연구”, 정보·보안논문지, 2011.

안황권, “시큐리티 환경변화에 따른 융합보안의 대두와 물리보안업체의 대응”, 정보·보안논문지, 2011

하옥현, “산업보안을 위한 융합보안관제시스템에 관한 연구”, 정보·보안논문지, 2009.

정수환, “융합보안 R&D 이슈 및 방향”, 정보보안학회논문지, 2009

한국산업기술평가관리원(2011.11), 2011년도 통합 산업기술수준조사 결과보고서

「공공기관의 개인정보보호에 관한 법률」법률 제8448호 법제명변경 및 일부개정
2007. 05. 17. (「공공기관의개인정보보호에관한법률」에서 변경)

「국가사이버안전관리규정」대통령훈령 제141호 신규제정 2005. 1. 31.

「벤처기업육성에 관한 특별조치법」법률 제8635호(자본시장과 금융투자업에 관한 법률) 일부개정 2007. 08. 03.

「벤처기업육성에 관한 특별조치법 시행규칙」산업자원부령 제397호 일부개정 2007.
4. 27.

「벤처기업육성에 관한 특별조치법 시행령」대통령령 제20261호(중소기업진흥 및 제품 구매촉진에 관한 법률 시행령) 일부개정 2007. 9. 10.

「전산망보급확장과이용촉진에관한법률」제정법률 제3848호 1986.5.12.

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」법률 제8486호 일부개정 2007.5.25.

「정보화촉진기본법」법률 제8031호 일부개정 2006.10.04.

「증권거래법」법률 제8527호 일부개정 2007.7.19.

「증권거래법 시행규칙」재정경제부령 제527호 일부개정 2006.11.08.

방송통신위원회 <http://www.kcc.go.kr/>

산업통상자원부 <http://www.motie.go.kr/>

한국사이버테러정보전학회 <http://www.kias.or.kr/>

한국정보보호산업협회(KISIA) <http://www.kisia.or.kr/>

한국인터넷진흥원(KISA) <http://www.kisa.or.kr/>

한국정보보호학회 <http://www.kiisc.or.kr/>

한국전자통신연구원(ETRI) <http://www.etri.re.kr/>

한국침해사고대응팀협의회 <http://www.concert.or.kr/>

한국CPO포럼 <http://www.cpoforum.or.kr/>

2 영문

- Gartner. Forecast: Information Security, Worldwide, 2015-2021. 2017
- Gartner. Forecast: Information Security, Worldwide, 2014-2020. 2016
- International Data Corporation(IDC). Worldwide Security Appliance Forecast and Analysis 2003-2007. 2003.
- International Data Corporation(IDC). Worldwide and U.S. Information Security Services. 2004-2008 Forecast. 2004.
- International Data Corporation(IDC). Worldwide Security Software 2004-2008 Forecast. 2004.
- International Data Corporation(IDC). Worldwide IT Security Software, Hardware, and Service 2006-2010. 2006.
- Lehman Brothers. Security Industry Annual Report 2003. 2003.
- J.P. Freeman "The 2008 U.S. Converged Security/IT Systems Market"



부 록

부 록 1	149
부 록 2	164
부 록 3	180



구분 1. 정보보안

대분류 1.1 정보보안 시스템 개발 및 공급

가. 네트워크보안 시스템 개발

인가되지 않은 노출, 변경, 파괴로부터 네트워크, 네트워크 서비스, 네트워크상의 정보를 보호하는 정보보호 활동을 총칭하며, 암호화, 전자서명, 접근통제, 데이터 무결성, 인증 교환 등의 보안 메커니즘을 활용한 정보보안 시스템.

네트워크 보안 제품으로는 웹방화벽, 네트워크(시스템) 방화벽, 침입방지시스템(IPS), DDoS 차단시스템, 통합보안시스템(UTM), 가상사설망(VPN), 네트워크 접근제어(NAC), 무선 네트워크 보안, 망분리(가상화), 차세대 방화벽(NGFW)이 있음.

웹방화벽(WAF: Web Application Firewall)은 네트워크 방화벽과 달리 OWASP(Open Web Application Security Project) Top10, 국가정보원의 8대 웹 취약점, 웹페이지 위변조 등 다양한 형태의 웹 기반 해킹 및 유해트래픽을 실시간 감시하여 탐지하고 차단하는 웹 애플리케이션 보안 솔루션임.

네트워크 방화벽은 네트워크 자산(서버 등) 구조의 최상단에 위치하며 인터넷과 같은 외부망으로부터 들어오는 접근 시도를 1차로 제어, 통제(허용/거부)함으로써 내부 네트워크를 보호하는 보안 솔루션임.

침입방지시스템(IPS: Intrusion Prevention System)은 네트워크 패킷을 분석하여 공격 시그니처(Signature)를 찾아내 제어함으로써 비정상적인 트래픽을 중단시키는 보안 솔루션임

수동적인 방어 개념의 방화벽이나 침입탐지시스템(IDS)과 달리 침입 경고 이전에 공격을 중단시키는데 초점을 둔 개념의 솔루션으로, 해당 서버의 비정상적인 행동에 따른 정보 유출을 자동으로 탐지하여 차단 조치를 취함으로써 인가자의 비정상 행위를 통제할 수 있음.

시스템 및 네트워크 자원에 대한 다양한 형태의 침입 행위를 실시간 탐지, 분석 후 비정상적으로 판단된 패킷을 차단해 네트워크 위협을 사전에 방지하는 시스템이라고 할 수 있음.

DDoS 차단시스템은 대량의 트래픽을 전송해 시스템을 마비시키는 DDoS(DDoS: Distributed Denial of Service, 분산서비스거부) 공격전용의 차단 솔루션으로, 이

제품은 대량으로 유입되는 트래픽을 신속하게 분석해 유해트래픽 여부를 판단해 걸러 줌으로써 보호대상 네트워크의 가용성과 안정성을 높여주며, 해당 서비스의 연속성을 보장하는 데 중요한 역할을 함.

통합보안시스템(UTM: Unified Threat Management)은 다중 위협에 대해 보호 기능을 제공할 수 있는 포괄적 보안 솔루션임. ‘통합보안어플라이언스’에 대한 IDC의 용어로서, UTM 보안 어플라이언스는 한 가지 이상의 보안기능 수행을 목적으로 개발된 하드웨어, 소프트웨어, 네트워킹 기술들의 결합체라고 규정하고 있음.

이 범주에 속하기 위해서는 어플라이언스가 반드시 네트워크 방화벽, ID&P, 게이트웨이 안티바이러스 기능들을 수행 가능해야 하며, 이 어플라이언스가 제공하는 기능들을 모두 사용하지 않을 수는 있지만 기능들은 반드시 어플라이언스 내에 포함돼야 하고, 이 제품 내에서는 개별 컴포넌트의 분리가 불가능함.

UTM이 제공하는 가장 주요한 장점으로 단순하고, 설치 및 사용이 간결하며, 모든 보안 기능이나 프로그램을 동시에 갱신할 수 있다는 점. 인터넷 위협의 특질과 다양성은 보다 복잡하게 발전하고 있기 때문에, UTM 제품 역시 이 모든 위협들에 대해 적절히 대응할 수 있도록 구성될 수 있어 시스템 관리자들이 오랜 기간에 걸쳐 다양한 종류의 보안 프로그램들을 유지, 관리해야 하는 수고를 덜어줌.

가상사설망(VPN: Virtual Private Network)은 인터넷망 또는 공중망을 사용하여 둘 이상의 네트워크를 안전하게 연결하기 위하여 가상의 터널을 만들어 암호화된 데이터를 전송할 수 있도록 만든 네트워크로 공중망 상에서 구축되는 논리적인 전용망임.

VPN은 모든 회사들이 개별적으로 회선을 임대하는 것보다 공중망을 공유함으로써 비용은 낮추면서도 전용회선과 거의 동등한 서비스를 제공하려는 것에서부터 출발하였음. 그래서 오늘날 가상사설망을 원하는 회사들은 주로 엑스트라넷(Extranet)이나 넓은 지역에 퍼져있는 지사들 간의 인트라넷(Intranet) 그리고 이동 사용자들의 안전한 원격접속(Secure Remote Access)에 VPN을 이용하고 있음.

네트워크 접근제어(NAC: Network Access Control)는 네트워크에 접근하는 접속 단말의 보안성을 강제화할 수 있는 보안 인프라로, 허가되지 않거나 웹·바이러스 등 악성코드에 감염된 PC 또는 노트북, 모바일 단말기 등이 회사 네트워크에 접속되는 것을 원천적으로 차단해 시스템 전체를 보호하는 보안 솔루션임.

무선 네트워크(Wireless Network) 보안이란 무선(전파)을 이용하는 통신 네트워크 상에서의 인증, 키 교환 및 데이터 암호화 등을 통해 위협으로부터 보호하기 위한 보안 솔루션임.

망분리는 조직에서 사용하는 망(네트워크)을 업무 및 내부용 망(인트라넷)과 외부망(인터넷)으로 구분하고 각 망을 격리함으로써 외부 위협으로부터 내부망을 보호하는 조치, 구성방식에 따라 완전히 분리된 두 개의 네트워크를 사용하는 물리적 망분리 방식과 가상네트워크, 가상 환경을 이용하는 논리적 망분리 방식으로 구분할 수 있음.

차세대 방화벽(NGFW: Next Generation Fire Wall)은 다양한 기능을 통합하고 더욱 고도화된 성능으로 업그레이드 된 방화벽으로 기존 방화벽과 구분하기 위해 사용되는 용어임.

가트너에 따르면 NGFW는 표준 방화벽 기능, 침입방지(IPS) 기능 및 애플리케이션 인식 및 제어기능을 포함하고 있다고 정의함.

즉, 차세대 방화벽은 단순히 정책(룰) 기반 트래픽 제어 기능뿐만 아니라, 위협 차단을 동적으로 수행하고 애플리케이션 레벨에 보안을 적용하는 기능까지 포함함.

나. 시스템보안 솔루션 개발

사용 허가권이 없는 사용자가 파일, 라이브러리 폴더 및 장치 등을 사용하지 못하도록 제한하여 보호하는 정보보안 시스템.

시스템 보안 제품으로는 시스템접근통제(PC방화벽 포함), 멀웨어 대응, 스팸차단 솔루션, 보안운영체제(Secure Operating System), APT 대응, 모바일 보안, 엔드포인트 탐지 및 대응(EDR), 랜섬웨어 대응이 있음.

시스템접근통제는 네트워크, 서버, IT 인프라 운영 시스템으로의 모든 접속과 작업을 통제·관리, 작업 모니터링, 로그기록 저장 등을 수행하는 보안 솔루션임.

시스템접근통제는 최근 서버 이외에 시스템의 해킹사고가 증가하고 있고 시스템 보안사고 대부분이 내부자에 의한 자료 유출 및 위·변조 등의 피해 사고로 그 필요성이 커지고 있음.

자료가 외부로 유출되는 것을 방지하기 위해 On-Line을 통한 파일유출 방지·감시 기능, SMTP-Mail, Web-Mail, Web-Hard, 게시판, FTP, Messenger, P2P Off-Line을 통한 파일유출 방지·감시기능, 프린터 인쇄 모니터링 기능, 그룹(공유폴더)접근 제어기능, 특정 소프트웨어 실행 차단 기능, 불법통신 및 사이트 차단 기능, 작업화면 스크린 캡처 기능 등 자료 유출을 보안하는 다양한 기능이 있음.

멀웨어 대응은 컴퓨터의 운영을 방해하거나, 정보를 유출 또는 불법적으로 접근권한을 취득하는 소프트웨어인 멀웨어를 방지하는 보안 솔루션임. 멀웨어는 독립적인 실행 파일 형식외에도 스크립트, 콘텐츠 등으로도 제작될 수 있으므로, 안티멀웨어는 바이러스(virus), 웜(worm), 트로이목마(Trojan horse), 루트킷(rootkit), 스파이웨어(spyware), 키로거(keylogger), 애드웨어(adware), 랜섬웨어(ransomware) 등 다양한 형태의 멀웨어로 인해 발생하는 공격에 대응함. 안티멀웨어 소프트웨어는 개인디바이스, 게이트웨이서버, 네트워크 어플라이언스 등에 설치 운영될 수 있음.

스팸차단 솔루션은 스팸전송자로 알려진 특정 이메일주소, 메일서버IP, URL, 제목과 내용, 대량전송 여부 등을 통해 스팸내용 및 불건전사이트 등을 검사하고 인식하여 차단하는 보안 솔루션임.

보안운영체제(Secure Operating System)는 컴퓨터 운영 체제의 보안상 결함으로

인하여 발생 가능한 각종 해킹으로부터 시스템을 보호하기 위해 기존의 운영 체제(OS) 내에 보안 기능이 추가된 운영 체제임.

서버의 보호, 시스템 접근 제한, 시스템 관리자에 의한 권한 남용 제한, 사용자의 권한 내 정보 접근 허용, 응용 프로그램 버그를 악용한 공격으로부터 보호 등이 요구되는 운영 체제임.

APT(APT: Advanced persistent Threat, 지능형지속공격)대응 솔루션은 APT공격에 대응하기 위한 보안 시스템임. APT는 의도가 분명한 악의적인 경제적 또는 정치적인 동기를 가지고 있고, 특정 기업이나 국가, 공공을 타겟으로 실행되는 은밀하고 지속적인 컴퓨터 공격 행위를 의미함.

APT대응 솔루션은 PC에이전트, 서버 소프트웨어, 어플라이언스 또는 그 조합으로 운영될 수 있음.

모바일 보안이란 모바일(휴대폰과 휴대용 개인정보단말기 등) 서비스(모바일 오피스, 모바일 बैं킹, 모바일 전자화폐 등) 상에 발생할 수 있는 위협(바이러스 공격, 개인정보 유출 등)으로부터 보호하기 위한 보안 솔루션임.

엔드포인트 탐지 및 대응(EDR: Endpoint Detection and Response) 솔루션은 패턴화돼 이미 알려져 있는 악성코드를 잡아내는 백신과 달리 신종 악성코드나 기존 바이러스가 변종돼 백신이 잡아낼 수 없는 악성코드까지 인지하고 이를 차단하는 보안 솔루션임.

기존 백신이 A위협, B위협을 각각 모니터링했다면, EDR은 통합적으로 이를 탐지하고 관리할 수 있는 역할까지 하게 돼 보안 사각지대를 줄일 수 있다는 장점이 있음.

최근 랜섬웨어 등 신종 보안 위협들이 갈수록 진화하면서, 정해진 사이버 공격 패턴만으로는 이를 감지하기가 쉽지 않아졌고 진화된 보안위협으로 보안 경계를 구분하는 것도 무의미해지면서 종합적인 대응할 수 있는 EDR의 필요성이 커지고 있음.

랜섬웨어(Ransomware)는 몸값을 의미하는 랜섬(Ransom)과 소프트웨어(Software)가 결합된 단어로, 사용자 pc의 자료들을 인질로 몸값을 요구하는 악성코드임.

랜섬웨어 대응 솔루션은 행위기반 분석기법 등을 통해 랜섬웨어 악성코드를 식별하여 사전차단하고, 데이터 백업을 통해 자료를 복구하는 기능 등을 포함함.

다. 정보유출방지 시스템 개발

디지털콘텐츠 불법 복제 및 유통 방지를 위한 기술적, 관리적 수단이나, 내부 기밀 정보의 유출을 탐지하고 차단하는 기능을 제공하는 정보보안 시스템.

콘텐츠/정보유출 방지보안의 제품으로는 DB보안(접근통제), DB암호, 보안USB, 디지털저작권관리(DRM), 네트워크 DLP, 단말 DLP가 있음.

DB보안(접근통제)은 데이터베이스 및 데이터베이스 내에 저장된 데이터를 인가되지 않은 변경, 파괴, 노출 및 비일관성을 발생시키는 사건으로부터 보호하는 보안 솔루션임.

DB암호는 데이터의 실제 내용을 허가받지 않은 사람이 볼 수 없도록 은폐하기 위해 데이터를 암호화하는 보안 솔루션임.

보안USB는 사용자식별, 지정데이터 암호·복호화, 지정된 자료의 임의복제 방지, 분실 시 데이터 보호를 위한 삭제 등의 기능을 지원하는 보안 컨트롤러가 있는 휴대용 메모리 스틱으로 보안 컨트롤러는 H/W, S/W로 구성될 수 있음.

디지털저작권관리(DRM: Digital Rights Management)는 웹을 통해 유통되는 각종 디지털 콘텐츠의 안전 분배와 불법 복제 방지를 위한 보안 솔루션임.

파일 교환 프로그램을 통해 전파되는 상업적 자료의 온라인 불법 복제로부터 디지털 콘텐츠를 보호하기 위한 것으로, 관련 법령이나 위반자 단속만으로는 예방이 어렵기 때문에 사후 단속 보다는 사전에 문제점을 파악해 첫 단계에서 내용 복제를 불가능하게 한 것임.

DRM 제품들은 서버 소프트웨어와 사용자 플러그인 운용에 필요한 패키지 제품들이 대부분임.

네트워크 DLP(DLP: Data Loss Prevention, 데이터유출방지)는 사용자의 고의 또는 실수, 외부 해킹, 멀웨어 등을 통해 네트워크를 이용한 정보유출을 콘텐츠 수준(Content-Aware)에서 막는 보안 솔루션임. 인터넷의 각종 통신(SMTP, HTTP/HTTPS, 인스턴트 메신저, 웹하드, SNS 등)을 통해 유출되는 정보의 내용을 감시하고, 필요에 따라 차단함.

단말 DLP(DLP: Data Loss Prevention, 데이터유출방지)는 사용자의 고의 또는 실수, 외부 해킹, 멀웨어 등을 통해 단말 호스트(PC, 서버, 모바일 등)에서의 정보유출을 콘텐츠 수준(Content-Aware)에서 막는 보안 솔루션임.

단말의 각종 외부 인터페이스(USB, 외장하드, CD/DVD, 프린트, 블루투스 TCP/IP 네트워크 등)를 통해 유출되는 정보의 내용을 감시하고, 필요에 따라 차단함.

라. 암호/인증 시스템 개발

암호는 평문을 제3자가 이해하기 곤란한 형식으로 변환하거나 암호문을 판독 가능한 형식으로 변환하는 원리나 수단, 방법 등을 다루는 기술임.

인증은 정보 교환에 의해 실제 식별을 확실하게 하는 방법으로 임의정보에 접근할 수 있는 객체의 자격이나 객체의 내용을 검증하는데 사용되는 수단으로 이를 통해 시스템의 부당한 사용이나 정보의 부당한 전송 등을 방어하는데 사용됨.

암호/인증 제품으로는 개인인증솔루션(OTP 포함), 공개키기반구조(PKI), 통합접근관리(EAM)/싱글사인온(SSO), 통합계정관리(IM/IAM)이 있음

개인인증솔루션(OTP 포함)은 로그인할 때마다 새로운 패스워드를 생성하는 보안 솔루션임. 패스워드를 반복 사용함으로써 생기는 패스워드 도난 문제를 예방함.

공개키기반구조(PKI: Public Key Infrastructure)는 실체의 식별자와 공개키를 포

합하는 정보로서 공개키 정보는 한 실체에 대한 데이터와 이 실체를 위한 공개키로 제한되며, 인증기관, 실체, 공개키 또는 관련된 알고리즘에 관한 다른 정적인 정보일 수 있음.

공개키 암호 기반기술의 집합체로써, 보안서비스에서 핵심적으로 필요한 비밀성, 무결성, 인증, 부인방지 기능 및 접근제어 기능을 제공하는 Application 계층의 데이터 보안 기술을 말함.

통합접근관리(EAM: Extranet Access Management)는 인트라넷, 엑스트라넷 및 일반 클라이언트/서버 환경에서 자원의 접근 인증과 이를 기반으로 자원에 대한 접근 권한을 부여, 관리하는 통합 인증 관리 솔루션임.

하나의 ID와 암호 입력으로 다양한 시스템에 접근할 수 있고 각 ID에 따라 사용 권한을 차등 부여하는 통합 인증과 권한을 관리할 수 있음.

일반기업과 금융권, 포털 등 기업 내 사용자와 일반 사용자에게 적용 가능하며 인터넷 뱅킹, 쇼핑 등 서비스 편의성과 운영비 절감 및 기업 내 보안 효과가 있음.

싱글사인온(SSO: Single Sign-on)은 이 기종의 시스템을 사용할 때마다 서로 다른 사용자번호(ID)와 비밀번호를 입력하지 않고도 한 번 인증만으로 전체 시스템을 하나의 시스템처럼 사용할 수 있도록 하는 솔루션임.

사용자가 전자상거래를 이용하기 위해 인터넷, 인트라넷 등 대내외 통신망에 접속할 때마다 ID와 패스워드를 각각 따로 지정해야 하는 번거로움을 없앴으며 사용자의 정보를 전자적으로 암호화해 파일로 저장한 신분증명서임.

통합계정관리(IM: Identity Management/IAM: Identity and Access Management)는 ID와 패스워드를 종합적으로 관리해 주는 역할 기반의 사용자 계정 관리 솔루션임. ID 도용이나 분실로 인한 보안 사고에 대비하여 보안 관리자에게는 사용자 역할에 따른 계정 관리, 사용자에게는 자신의 패스워드에 대한 자체 관리 기능을 제공함.

또한 시스템과 각종 자원에 대해 고객·기업 내 사용자·관리자 등의 접근을 제어할 수 있어, 한 번의 ID와 패스워드 입력으로 다양한 시스템에 접속할 수 있도록 싱글사인온(SSO)이나 ID에 따라 사용 권한을 차등적으로 부여하는 엑스트라넷 접근관리(EAM)를 확장 또는 보완한 것임.

마. 보안관리 시스템 개발

비인가된 접근으로부터 통신네트워크 및 시스템, 응용서비스 등을 보호하기 위한 관리 기능을 갖춘 제품으로 보안 서비스와 메커니즘의 생성, 제어, 삭제 기능, 보안 관련 정보의 분배 기능, 보안 관련 이벤트의 보고 기능, 암호키의 분배제어 기능, 인가된 사용자의 접근권한 관리 기능 등 다양한 서브기능들이 포함.

보안 관리 제품으로는 통합보안관제시스템(SIEM), 위협관리시스템(TMS), 패치관리 시스템(PMS), 백업 및 복구관리시스템, 로그관리 및 분석시스템, 취약점 분석 시스템,

디지털 포렌식 시스템이 있음.

통합보안관제시스템(SIEM: Security Information and Event Management)은 방화벽, 침입탐지시스템, 가상사설망 등 각종 보안시스템 및 주요시스템 장비를 연동하여 효율적으로 운영할 수 있도록 하는 통합보안관리 솔루션임.

최근에는 통합관리 수준에서 벗어나 시스템 자원 관리(SMS: System Management System), 망 관리시스템(NMS: Network Management System)등 기업보안관리시스템에까지 확대·개발되고 있음.

기업보안관리는 기업들이 서로 다른 기종의 보안솔루션 설치에 따른 중복투자, 자원 낭비를 줄일 수 있으며, 솔루션 간 상호 연동을 통해 네트워크상에서 발생하는 유해트래픽 정보를 분석하여 다양한 위협에 대한 사전·후 대응을 가능하게 해 줌은 물론, 전체 정보통신시스템에 대한 보안 정책을 수립할 수 있다는 장점이 있음. 즉, 일관된 정책으로 네트워크상에 산재해있는 이기종 보안장비(방화벽, IDS, IPS, VPN 등)와 네트워크 장비(서버, 라우터 등)를 통합하여 효율적으로 운영하고 관리할 수 있도록 지원해주는 솔루션이라고 볼 수 있음.

위협관리시스템(TMS: Threat Management System)은 국내외 최신 취약성 정보와 보안 트렌드, 정밀 분석된 네트워크 트래픽 및 공격 형태를 상관 분석해 인터넷 웹, 바이러스, 해킹 등의 사이버 공격을 예측하고 판단하여 보다 능동적으로 대응할 수 있는 체계적인 위협관제 및 대응 솔루션임.

패치관리시스템(PMS, Patch Management System)은 시스템의 보안 취약점을 보완하기 위하여 배포되는 보안 패치 파일을 원격에서 자동으로 설치, 관리해 주는 솔루션임.

보안 패치의 미설치로 인해 발생할 수 있는 각종 피해를 예방하기 위해 패치 설치를 권고하여 설치를 유도하거나, 필요시 강제적으로 설치할 수 있도록 관리함. 웹·바이러스 등 사이버 위협에 대한 효과적인 해결책의 하나로 제시되어 공공기관을 중심으로 도입이 확산되고 있음.

백업 및 복구관리시스템은 자료 손실을 예방하기 위해 자료를 미리 다른 곳에 임시로 보관해 두었다가 원래 상태로 복구해주는 관리 솔루션임.

로그관리 및 분석시스템은 서버, 네트워크장비, 어플리케이션 등의 IT인프라에서 발생하는 다양한 로그를 실시간으로 수집, 저장, 모니터링 및 분석하는 등의 작업을 위해 사용되어지는 솔루션임.

취약점 분석 시스템은 악성코드 민감도, 안전하지 않은 소프트웨어 설정, 열린 포트 같은 컴퓨터 시스템의 알려진 취약점들을 분석하기 위해 사용되어지는 보안 솔루션임.

디지털 포렌식 시스템은 정보기기 내에 내장된 디지털 자료를 법적 증거가 되도록 하기 위해 자료를 수집, 보관, 분석, 보고하기 위해 사용되어지는 보안 솔루션임.

대분류 1.2 정보보안 관련 서비스

바. 보안컨설팅 서비스

조직의 목적을 달성하는데 있어 전산시스템과 네트워크 등 모든 IT 자산과 조직에 일어날 수 있는 위험을 분석하고 이에 대한 대책을 수립함으로써 관리자와 조직이 그 대책을 실현할 수 있도록 지원하는 독립적인 전문자문 서비스.

보안컨설팅 서비스로는 정보보호 평가/인증(ISO/ISMS/CC 등), 진단 및 모의해킹, 개인정보보호컨설팅, 정보감사(내부정보유출방지컨설팅 등), 기타 보안컨설팅(기반보호, 보안SI 포함)이 있음.

정보보호 평가/인증(ISO, ISMS, CC 등)은 조직이 수립 및 운영하는 관리체계가 정보보호 측면에서 적합한지를 판단하는 제도로 인증을 통해 정보보호 관리에 대한 인식을 제고해 보호해야할 정보통신망 및 정보자산의 안전성과 신뢰성을 향상시키는 것이 목적임.

정보보호 관리체계(Information Security Management System)란 조직에 적합한 수준의 정보보호를 제공하기 위해 정책 및 조직을 수립하고 위험관리, 대책 구현, 사후 관리 등의 정보보호 관리과정을 통해 여러 정보보호대책들이 유기적으로 통합되어 구현, 운영되는 체계임. 각 조직들은 ISMS 구축을 통해 보유하고 있는 정보자산의 기밀성·무결성·가용성을 실현하여, 보다 효율적이고 효과적인 방법으로 보유 정보들을 보호함.

CC(CC: Common Criteria, 공통평가기준)인증제도는 민간업체 등에서 개발한 정보보호시스템을 국제표준인 ISO15408 및 ISO18045를 이용하여 보안기능에 대한 안정성과 신뢰성을 보증함으로써 사용자들이 안심하고 정보보호시스템을 사용할 수 있도록 지원하는 제도임.

진단 및 모의해킹은 인가 받은 해킹 전담 컨설턴트에 의해 외부 또는 내부 네트워크 상에서 실제 해커가 사용하는 최신 해킹기법 및 도구를 이용하여 네트워크, 서버 및 응용 프로그램의 취약점을 통해 정보 시스템으로의 침투 가능성을 진단하는 ‘Ethical Hacking’임. 모의해킹을 통해 서버, 네트워크, 어플리케이션 상에 존재하는 취약점들을 심층적으로 분석함으로써 현재의 보안수준을 평가하고 이에 대한 종합적인 대응책과 권고안을 제시하여 보안성을 강화하는 것이 목적임.

개인정보보호컨설팅이란 온라인상에서 개인의 신용정보 등 중요한 개인정보를 보호하는 것을 목적으로 개인의 허락 없이 개인의 정보가 유출되어 도용되는 것을 방지하기 위한 보안 컨설팅 서비스임. 개인의 명의를 도용되어 사용하는 것을 막고 주민등록번호를 이용한 사이트 이용이나 계좌거래 등을 방지하기 위해 개인신상정보가 노출되지 않도록 차단 및 진단, 관리기능을 수행함.

정보감사는 사용자의 정보 흐름을 추적하여 고객정보, 핵심기술, 영업정보 등 기업

의 내부 중요정보가 전산시스템, 사람 등에 의해 유출 될 수 있는 위협 및 가능성을 분석하고 이에 대한 대책을 수립하고 관리함으로써 기업정보 유출 방지를 지원하는 보안 컨설팅 서비스임.

기반보호 컨설팅이란 전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립·시행함으로써 동 시설을 안정적으로 운용하도록 하여 국가의 안전과 국민생활의 안정을 보장하는 보안 컨설팅 서비스임.

주요정보통신기반시설은 국가안정보장, 행정, 국방, 금융, 통신, 운송, 에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 정보통신망 등을 말함

보안SI(SI: System Integration)는 보안 솔루션 및 인프라를 구축하는 서비스임.

사. 보안시스템 유지관리/보안성 지속 서비스

보안시스템 유지관리는 사용자가 구매한 정보보안 제품을 최적의 상태에서 활용, 유지할 수 있도록 하기 위해 제공되는 제품지원, 기술지원, 사용자 지원 등의 서비스임.

보안성 지속 서비스는 정보보안 제품을 활용하여 정보의 훼손, 변조, 유출 등을 방지하기 위해 지속적으로 요구되는 기술기반의 서비스로, 사이버위협에 따른 보안업데이트, 보안정책관리, 위험·사고분석, 보안성 인증효력 유지, 보안기술자문 등으로 구분됨.

아. 보안관제 서비스

보안관제서비스(MSS: Managed Security Service)는 고객의 IT자원 및 보안시스템에 대한 운영 및 관리를 전문적으로 아웃소싱(outsourcing)하여 각종 침입에 대해 중앙관제센터에서 365일 24시간 실시간으로 감시 및 분석, 대응하는 서비스임.

정보자산에 대한 보안은 전문 보안업체에 아웃소싱하고, 고객은 자신의 핵심 역량에 집중할 수 있는 선진화된 보안 서비스임.

보안관제 서비스에는 보안기업의 관제센터에서 고객사의 보안시스템을 원격으로 운영·관리하는 원격관제 서비스, 보안관제기업의 인력이 고객사에 상주하여 서비스를 제공하는 파견관제 서비스가 있음

원격관제 서비스는 보안기업의 관제센터에서 고객사의 보안 시스템을 원격으로 운영, 관리하는 형태로 별도의 회선 구축 없이 인터넷망을 통한 관제가 가능해 운영 부담을 낮출 수 있음.

파견관제는 보안관제 인력이 고객사에 상주하여 서비스를 제공하는 방식으로, 해당 고객사에 특화된 관제 서비스를 제공할 수 있고 침해/장애 발생 시에도 즉각적인 조치가 가능함.

자. 보안교육 및 훈련 서비스

정보보안에 대한 다양한 교육훈련 프로그램을 통해 대학생, 기업 보안 관리자의 전문성 강화와 기업 내 임직원들의 정보보안에 대한 인식 강화를 통해 각 기관의 전반적인 보안수준을 향상시킬 수 있음.

차. 공인/사설 인증서

공인/사설 인증은 통신망을 통하여 컴퓨터에 접속하는 사용자가 등록되어 있는 정당한 사용자인지의 여부를 신뢰할 수 있는 방법으로 개방형 망에서 특히 중요함.

중심 부분은 인증 서버라는 소프트웨어로 사용자의 이름과 패스워드 등을 일괄 관리하며, 인증 서버는 서비스를 제공하는 프로그램에 대해서 패스워드를 이용한 인증용의 프로토콜을 사용하여 사용자가 허가를 받은 본인이라는 사실을 인증함.

구분 2. 물리보안

대분류 2.1 물리보안 시스템 개발 및 공급

가. 보안용 카메라 제조

영상 촬영이 가능한 장치로, 아날로그 카메라(저해상도), 아날로그 HD 카메라(고해상도), 네트워크(IP) 카메라, 특수카메라(열화상/3D 카메라 등) 등이 있음.

아날로그 카메라(저해상도)는 네트워크 기능이 불가능하여 CCTV카메라를 연결하고 있는 DVR에만 영상을 전송하고 저장하는 카메라로 보통 VGA(640×480)급 해상도의 카메라를 의미함.

아날로그 HD 카메라(고해상도)는 아날로그 카메라로 기존 동축케이블을 그대로 사용하지만 화질이 고해상도로 최대 Full HD (1080p)해상도를 지원함. DVR역시 AHD 용 DVR을 사용하여야 하며 기존 아날로그 DVR과는 호환되지 않음.

네트워크(IP) 카메라는 유무선 랜에 연결하여 사용하는 카메라임. 카메라 모듈, 디코더, 영상 압축 칩, CPU, 네트워크 전송 칩 등으로 구성되며, 카메라 모듈로부터 받은 아날로그 신호는 디코더를 통해 디지털로 바뀌고, 압축 칩에서 압축을 거쳐 네트워크로 전송됨.

특수카메라인 열화상 카메라는 온도에 따라 다른 색으로 표현하여 우리 눈으로 그 온도를 볼 수 있게 한 카메라이다. 이 열화상 카메라는 여러 가지 용도로 사용된다. 열화상 카메라로 열이 전달되는 것을 관찰할 수 있다.

3D 카메라는 특정 장면에서 객체에 작용하는 모든 광선을 수집해 객체의 심도(깊이의 정도) 정보를 포착할 수 있는 카메라로 입체감을 인식할 수 있는 영상 출력이 가능함.

나. 보안용 저장장치 제조

카메라에 의해 촬영된 영상정보를 저장, 관리하는 장치로 임베디드 운영체제 내장 DVR(Digital Video Recoder), PC/서버 기반 DVR(Digital Video Recoder), 운영체제 내장 NVR(Network Video Recorder), PC/서버 기반 NVR(Network Video Recorder), 백업스토리지(콜드스토리지) 등이 포함됨.

임베디드 운영체제 내장 DVR은 DVR 기능 구현을 위해 전용 하드웨어를 설계, 개발한 제품으로 DVR 기능구현에 필요한 부품만 사용하므로 가격이 저렴하며, 또한 Embedded OS를 사용하므로 윈도우를 사용하는 PC기반 DVR보다 안정적인 환경을 제공함.

PC/서버 기반 DVR은 PC에서 사용하는 메인보드, CPU를 그대로 활용하고 영상압축을 위한 캡처보드를 장착해 사용하는 제품을 말함.

운영체제 내장 NVR은 NVR기능 구현을 위해 전용 하드웨어를 설계, 개발한 제품으로 Embedded OS를 사용하므로 윈도우를 사용하는 PC기반 NVR보다 안정적인 환경을 제공함. 별도의 CPU 없이 DSP를 기반으로 하여 하드웨어를 구동시켜야 하기 때문에 상대적으로 높은 기술적 난이도가 존재함.

PC/서버 기반 NVR은 네트워크 상에 설치된 네트워크 카메라나 비디오 서버 영상의 녹화, 모니터링, 이벤트 관리, 재생 등을 위한 전용 소프트웨어가 설치된 PC 서버를 말함.

IP 카메라를 통해 디지털 영상을 전송받아 압축 저장하는 기능으로, IP 전용 저장장치이기 때문에 아날로그를 디지털로 변환하는 장치가 필요 없고 기존 디지털 비디오 녹화기(DVR)를 대체하는 장치임.

백업스토리지는 IT시스템에 문제가 발생하였을 때 필요한 백업 데이터를 저장하는 별도의 장치이며, 콜드스토리지는 에너지 절감을 위해 연산 능력에서 약간의 손해를 보더라도 낮은 가격과 낮은 전력으로 자주 사용되지 않는 데이터를 처리하는 데이터 저장장치 및 시스템임.

다. CCTV 카메라 부품

카메라를 구성하는 렌즈 및 영상데이터를 변환하는 집적회로, 이미지 센서 등 영상장치를 구성하는 부품을 포함하며, 칩셋(코덱칩, 콘트롤칩), CCTV렌즈, 기타 부품(모듈/CCD/CMOS/보드 등)이 있음.

칩셋은 컴퓨터 메인보드에 설치된 대규모 집적회로군의 말하며, 코덱(coder/decoder)이라는 용어는 데이터 변환을 수행하는 집적회로나 칩과 관련하여 사용됨. 코덱의 형태는 아날로그-디지털 변환이나 디지털-아날로그 변환기능이 하나의 칩 내에 결합되어 있음.

CCTV렌즈는 CCTV카메라 제조에 사용되는 카메라 렌즈모듈을 의미하며, 렌즈는 카메라가 촬영하는 피사체를 화면에 어느 정도의 크기로 할지, 수동여부, 밝기 화면에 대해 조리개를 자동으로 제어할지 여부, 줌 필요성, 원격제어 필요성 등에 따라 선택함. 일반적으로 고정초점렌즈와 가변초점 렌즈, 줌 렌즈 등 크게 3그룹으로 분류됨.

기타 부품의 CCD(Charged Coupled Device)는 빛 에너지를 전기적인 신호로 변환하는 수천만 화소를 포함하는 집적회로가 내장된 이미지 센서로서 원화상을 광학계를 이용해 고체소자에 결상시켜 그 상을 고체소자 내에서 전자적으로 주사하여 전기신호로 변환해 출력하는 소자를 말함.

CMOS(Complementary Metal Oxide Semiconductor)는 상보형 금속산화 반도체라는 뜻으로 컴퓨터에서 배터리에 의하여 동작되는 기억 장치로써 컴퓨터 시스템의 구성 정보를 보관하는 기억 장소의 재료로 사용되고 있음.

라. 물리보안 솔루션

영상기기를 통해 수집된 정보를 통합 감시 관리하는 시스템으로 영상감시관제 SW(CMS, VMS)와 지능형 영상감시 솔루션 등이 있음

영상감시관제SW에서 중앙관리시스템(CMS; Central Monitoring System)은 PC 한 대에 모든 프로그램을 설치하는 시스템으로 사용자수에 따라 화질에 영향을 받으며, SW를 주로 번들로 제공하는 경우가 많음. 영상관리시스템(VMS; Video Management System)은 개방, 분산형 보안관리 시스템으로 어떠한 경우에도 설정한 화질을 유지하며, 전문적인 영상 관리 SW로 취급됨.

CMS는 최대 통합 가능한 채널이 120여개에 그치나 VMS는 최대 1만대 이상의 영상기기를 통합 관리할 수 있으며, 서버-클라이언트 구조로 이뤄져 네트워크 감시카메라와 영상전송 서버 등을 통합해 관리하고, 각종 센서와 오디오 등을 연동할 수 있는 상용 소프트웨어임.

지능형 영상감시 솔루션은 사람의 감각을 통해 진행되던 기존의 CCTV 영상감시의 한계를 극복하고자, CCTV의 영상을 소프트웨어와 하드웨어를 통해 각종 객체(사람, 사물 등)를 구분하고 움직임을 판단하는 자동화된 솔루션임.

마. 물리보안 주변장비

영상기기 외에 자료의 전송, 변환, 출력 등을 지원하는 주변장비로 영상전송/변환장비 및 모듈(비디오서버, 암호화 장비, 무선통신용 모듈 등), 보안용 모니터, 전용부품(하우징/브라켓/폴대 등)이 있음

영상전송/변환장비 및 모듈은 기존에 구축된 아날로그 카메라를 IP 기반으로 전환하고자 할 경우에 많이 사용됨. 아날로그 카메라가 비디오 서버에 연결되면 압축 프로세서를 통해 디지털로 전환 처리되며, 비디오 서버는 네트워크에 연결되고, 네트워크 스위치를 통해 PC로 전송됨. 웹 트랜스미터라고도 하지만 전세계적으로 “비디오 서버”라는 명칭을 공통으로 사용하고 있음.

보안용 모니터는 일반적인 PC용 모니터가 지원하지 않는 PC VGA 출력 화면을 디스플레이 하는 게 주목적으로, 보안감시용 시장에서 요구하는 다채널 입력 및 Loop Through Output 기능 등을 지원하지 않음. 무엇보다 아날로그 VCR 및 스탠드얼론 DVR 출력과의 호환성 지원 때문에 CCTV 전용 모니터가 필요함.

전용부품은 카메라를 광선으로부터 보호하거나 방수 기능을 하는 커버케이스, 건물 벽면 설치 시 거치대, 지지대, 설치기둥 등의 각종 CCTV 액세서리를 의미함.

바. 출입통제 장비 제조

주요 관공서, 군 주요시설, 금융기관, 회사, 연구실 등의 보안유지가 요구되는 곳, 또

는 이용자의 출입관리가 요구되는 곳에서 ID CARD 등의 인식장비를 활용하여 관리하는 시스템을 말함. 카드&리더(번호/마그네틱), 컨트롤러, 시큐리티게이트 등이 있음.

사. 생체인식 보안시스템 제조

사람의 지문이나 얼굴 등 신체적인 특징 또는 서명하는 동작이나 걸음걸이 등 개인의 행동적 특징을 이용하여 신원을 확인하는 기술.

해당 제품으로는 얼굴인식시스템, 지문인식시스템, 홍채인식시스템, 정맥인식시스템, 기타(음식인식 및 기타)가 있음.

얼굴인식시스템은 사람 얼굴의 대칭적인 구도, 생김새, 머리카락, 눈의 색상, 얼굴 근육의 움직임 등을 분석해 얼굴의 특징을 알아내는 대표적인 생체인식 기술임.

지문인식시스템은 전용 센서를 이용해 지문의 디지털 영상을 획득하여 지문에 있는 다양한 패턴을 이용하여 신원을 확인하는 기술임.

홍채인식시스템은 홍채의 모양과 색, 망막 모세혈관의 형태소 등을 분석해 사람을 인식하는 생체인식 기술임.

정맥인식시스템은 손바닥이나 손가락에 흐르는 정맥을 이용해 본인 여부를 인식하는 생체인식 기술임.

기타로 사람 목소리의 특성을 인식하는 기술 및 상기분류에서 제외된 바이오인식 시스템이 있음.

아. 경보/감시 장비 제조

적외선/레이저/진동/장력 센서, 모션디텍터/침입탐지장비 센서 등을 활용하여 온도, 압력, 방사선 세기 등의 물리량이나 화학량을 검지하여 신호 처리가 가능하도록 변화시키는 장치로 방범이나 화재 감시 등에 널리 사용되고 있으며, 의료용 서모그래피, 동식물의 생태 관찰 등으로 응용이 확대되고 있음.

자. 기타제품

해당 분류에 포함되지 않는 기타 제품.

블랙박스는 내부의 룸미러 근처나 대시보드 등에 설치해 영상 데이터를 촬영, 동영상으로 기록하는 카메라 형식의 제품임.

대테러장비(볼라드, X-레이검색, 타이어킬러, 차량하부스캐너 등)에는 911 테러 이후 홈랜드시큐리티에 대한 논의가 이루어지면서 탄생한 로드블록, 타이어킬러와 같은 대테러장비, 주요 시설물 주변에 설치하는 볼라드 등이 있음.

대분류 2.2 물리보안 관련 서비스

차. 출동보안 서비스

사람이 아닌 CCTV, Access Control 등의 기계를 설치하여, 이상 감지시 경보를 울리고, 상황을 알려서 신고를 하거나 인력을 설치된 현장으로 보내는 서비스.

카. 영상보안 서비스

출동보안 서비스에서 인력의 출동을 제외한 CCTV 및 센서 등의 설치를 통해 현장의 영상을 여러 종류의 Device를 통해 제공해 주는 보안영상 제공 서비스(출동 서비스 제외).

타. 기타보안 서비스

현재, 통신 사업자 및 망 사업자들이 자신들의 인프라를 이용해서 IP카메라의 영상을 IDC와 같은 곳에 저장하여 각 개인이 집 등에 대한 영상을 볼 수 있도록 제공해주는 서비스가 대표적이며, 외에도 보안과 관련된 서비스를 포함(설치 및 유지관리 포함).

부록2

2019년 정보보호산업 실태조사 설문지



승인번호
제 127013 호

2019년 국내정보보호산업 실태조사

안녕하십니까? 귀사의 무궁한 발전을 기원합니다.

과학기술정보통신부와 한국정보보호산업협회가 공동으로 진행하는 본 조사는 정보보호산업진흥법 시행령 제20조(통계의 작성)에 의거하여 국내 정보보호산업 발전을 위해 정확한 실태를 파악하고 동 산업의 문제점과 개선방안을 발굴해내기 위한 것으로, 본 자료는 과학기술정보통신부 등 유관기관에서 정책을 수립하고 집행하는데 중요한 기초정보로 활용됩니다.

통계의 신뢰성과 정확성 확보를 위해 정보보호기업 여러분의 적극적인 협조가 필요합니다.

아울러 작성해 주신 자료는 반드시 조사와 연구에 관련된 목적에만 사용될 것이며, 비밀은 철저히 보장될 것임을 약속드립니다. 설문조사에 응해주셔서 감사합니다.

- 조사기관 : 한국정보보호산업협회(KISIA)

※ 본 조사의 신뢰도와 정확성을 기하기 위해 귀사 대표이사(또는 경영관리 부서장) 책임 하에 설문응답 바랍니다.

※ 8월 30일 이내에 회신주신 기업에 한하여 백화점 상품권(모바일 전용)을 보내드릴 예정이오니, 적극적인 설문 부탁드립니다.

2019. 8.

과학기술정보통신부·한국정보보호산업협회

해당 사업 분야	정보보안 ()		물리보안 ()		* 해당분야 중복 체크 가능.
대표 응답자 정보				응답 확인자(담당 부서장)	
성명		전화번호		성명	
부서/직위		e-mail		부서/직위	
답례품 발송 휴대폰 번호				전화번호/e-mail	

□ 정보보안 기업용

I. 귀사의 일반현황에 관한 질문입니다.

회 사 명		설립년도	년	사업자등록번호				
대표이사 성명		대표이사 E-mail		종업원 수 (2018년 12월)	명	남자	명	
소 재 지	①서울 ②부산 ③대구 ④인천 ⑤광주 ⑥대전 ⑦울산 ⑧경기 ⑨강원 ⑩충북 ⑪충남(세종) ⑫전북 ⑬전남 ⑭경북 ⑮경남 ⑯제주					여자	명	
자본금	자본금: 백만원			보안인력 수 (2018년 12월)	명	남자	명	
기업 형태	준거법 기준 1. 내국회사 2. 외국회사 자본구성 기준 1. 내자회사 2. 외자회사 3. 합작회사					매출 현황	연간 총매출액	2018년
상 장 여 부	1. 비상장 2. 코스닥 3. 거래소 4. 코넥스			매출 현황	연간 총매출액			2019년(추정)
일반/벤처기업	1. 일반기업 2. 벤처기업					매출 현황	연간 총매출액	2018년
주사업 분야	1. 정보보호(정보보안/물리보안)사업이 주사업 2. 타사업이 주사업			매출 현황	연간 총매출액			2019년(추정)
주력제품/서비스	*첨부 '정보보호산업 분류표'를 참고하여 작성					2018년 수요처별 정보보안 매출비중(%)		공공/교육

II. 귀사의 매출현황에 관한 질문입니다.

※ 총계는 2페이지의 2018년, 2019년 정보보안 총매출액과 같아야 합니다.

※ 2019년 총매출은 상반기(6월말 기준 실적액)와 하반기(7월 이후 12월말 기준 추정액) 합계

귀사에서 취급하는 정보보안 제품 또는 서비스를 분류표(첨부자료- 19페이지 참고)에 따라 작성해주시고, 각각의 해당사항에 대해 숫자로 기입하여 주십시오.				총 매출액 (단위: 백만원)		
대분류	중분류	제품 및 서비스	2018년 매출액	2019년 매출액 (1월~6월)	2019년 매출액 추정 (7월~12월)	
총 계 (S/N 정보보안+서비스)*						

국내 정보보호산업 실태조사
2019

1. 귀사는 4차산업관련 제품을 현재 개발 혹은 출시하고 있습니까? ()
 1) 있음, 이미 출시 2) 있음, 현재 개발 중임 3) 없음, 계획없음

1-1. 1)의 응답자의 경우, 현재 귀사에서 개발·활용하고 있는 4차 산업혁명 관련 기술 분야는 무엇입니까?

구분	관련 제품명	2018년 매출액 (단위: 백만원)	2019년 추정매출액 (단위: 백만원)
1.클라우드			
2.사물인터넷			
3.빅데이터			
4.인공지능			
5.블록체인			

2. 귀사의 2019년 매출은 작년과 비교하여 얼마나 악화 또는 호전이 예상됩니까?

	악화가 예상된다 ----- 비슷하다 ----- 호전이 예상된다				
2. 2019년 매출	①	②	③	④	⑤

2-1. 귀사의 2019년 매출이 작년 대비 악화 또는 호전이 예상되는 이유는 무엇입니까?

()

3. 귀사의 2020년 매출은 올해와 비교하여 얼마나 악화 또는 호전이 예상됩니까?

	악화가 예상된다 ----- 비슷하다 ----- 호전이 예상된다				
2. 2019년 매출	①	②	③	④	⑤

3-1. 귀사의 2020년 매출이 작년 대비 악화 또는 호전이 예상되는 이유는 무엇입니까?

()

III. 귀사의 수출현황에 관한 질문입니다.

※2019년 예상액은 상반기(6월말기준 실적액)와 하반기(7월이후 12월말기준 전망액) [단위: 백만원, %]

귀사에서 취급하는 정보보안 제품 또는 서비스를 분류표(첨부자료- 19페이지 참고)에 따라 작성해주시고, 각각의 해당사항에 대해 숫자로 기입하여 주십시오.			수 출			2018년 국가별 수출비중 (각 국가의 합 100%)				
대분류	중분류	제품 및 서비스	연도별 수출액 및 예상액 (단위: 백만원)			국가명(직접기입)				
			2018년 수출액	2019년 수출액 (1월~6월)	2019년 수출액추정 (7월~12월)					
						%	%	%	%	%
						%	%	%	%	%
						%	%	%	%	%
						%	%	%	%	%
						%	%	%	%	%
						%	%	%	%	%
						%	%	%	%	%
						%	%	%	%	%
						%	%	%	%	%
						%	%	%	%	%
총 계 (S/N 정보보안+서비스)*										

1. 귀사에 해외로 진출하고 싶은 정보보안 제품 또는 서비스가 있다면, 무엇이고 진출하고 싶은 국가는 어디입니까?

대분류	중분류	제품 또는 서비스	희망 진출국가

2. 귀사의 2019년 수출은 작년과 비교하여 얼마나 악화 또는 호전이 예상됩니까?

	악화가 예상된다 ----- 비슷하다 ----- 호전이 예상된다				
2. 2019년 수출	①	②	③	④	⑤

2-1. 귀사의 2019년 수출이 작년 대비 악화 또는 호전이 예상되는 이유는 무엇입니까?

()

3. 귀사의 2020년 수출은 올해와 비교하여 얼마나 악화 또는 호전이 예상됩니까?

IV. 귀사의 수입 현황에 관한 질문입니다.

1. 귀사에서는 정보보안 분야에서 2018년도나 2019년도에 해외로부터의 수입이 있었습니까?

① 있었음 => 2번으로 이동

② 없었음 => V. 기술인력/고용 파트로 이동

2. 귀사가 2018년과 2019년에 수입하였거나 수입이 예상되는 금액, 수입국가를 간략하게 기술하여 주시기 바랍니다.

* 외국으로부터 직접 완제품, 반제품을 구매한 것으로 응답기업체가 수입신고필증 상 수입자로 되어있으며, 과세가격으로 표기된 금액

	2018년 수입액	2019년 상반기 수입액 (1월~6월)	2019년 하반기 수입액 (7월~12월)	2018년 수입국가
정보보안	백만원	백만원	백만원	

V. 귀사의 기술인력/고용 현황에 관한 질문입니다.

1. 귀사의 전체 종업원 수를 전공(최종학력 기준)으로 나누어 해당 칸에 기입하여 주십시오.(2018년 12월 말 기준)

구분	전공 학과	합계
1) 정보보안(호)과	정보보안(호)학과	명
2) 정보보안(호) 관련학과	전자 관련학과, 통신 관련학과, 컴퓨터 관련 학과 등	명
3) 비관련학과	인문, 사회계열, 예·체능계열 등 정보통신 비관련학과 등	명
전체 합계(총 종업원 수)		명

* 전체 합계는 2페이지의 2018년 12월 기준 총 종업원 수의 합계와 같아야 합니다.

2. 2018년 12월말 기준, 귀사의 총 종업원 중 정보보안 관련 기술 및 연구인력 종사자를 구분하여 해당 칸에 기재하여 주십시오.

구 분	세부분류	세부 직종 예시	인원
정보보안 연구 및 개발	시스템 및 네트워크 기술, 암호 및 인증, 기술응용기술 및 서비스	- 컴퓨터시스템 분석 및 설계 전문가·네트워크 분석 및 설계 전문가 - 관련 연구소 및 산업체의 연구원·컴퓨터 악성프로그램 분석가	명
엔지니어	정보시스템 관리	- 데이터베이스 관리자(DB운영)·OS 운영자·리눅스 전문가 - 전산관리 전문가·시스템 엔지니어·CIO/CSO/CISO	명
정보보안 관리	정보보안 컨설팅	정보보안 컨설턴트	명
	정보보안 관제	정보보안 관제	명
정보보안 영업	정보보안 마케팅	정보보안제품 마케팅, 국내외 판로확보	명
기타 정보보안 관련직	정보시스템 감리 및 인증, 정보보안 교육, 기타	- 정보시스템 감사사·관련 학과를 개설한 대학의 교수 - 관련 사설교육기관의 강사·기타 정보보안 업무 관련자	명
전체 합계(총 보안 인력)			명

* 2018년 12월 기준 정보보안 인력의 전체합계는 2페이지의 해당년도 총 보안인력 수와 같아야 합니다.

3. 2018년 12월말 기준, 귀사의 총 종업원 중 정보보안 관련 기술 및 연구인력 종사자를 경력으로 구분하여 해당 칸에 기재하여 주십시오.

구 분	인원
정보보안 관련 경력 4년 미만	명
정보보안 관련 경력 4년 이상 7년 미만	명
정보보안 관련 경력 7년 이상 11년 미만	명
정보보안 관련 경력 11년 이상 15년 미만	명
정보보안 관련 경력 15년 이상	명
전체 합계(총 보안 인력)	명

* 2018년 12월 기준 정보보안 인력의 전체합계는 2페이지의 해당년도 총 보안인력 수와 같아야 합니다.

4. 정보보안 관련 인력을 채용했거나 채용할 계획이 있습니까?(채용하지 않았거나 계획이 없는 경우, '0'으로 표시)

	2019년(상반기 채용 및 하반기 예상)	2020년 (채용 계획)
신입	명	명
경력	명	명
합계	명	명

VI. 귀사의 기술/연구개발 및 기업 경쟁력 관련 질문입니다.

1. 귀사는 기술개발 관련 자체기술연구소나 전담부서를 운영하고 있습니까?

- ① 기업부설연구소 운영(명) ② 연구개발전담부서 운영(명) ③ 없음

2. 귀사의 정보보안산업 관련 전체 투자액 및 연구개발 관련 투자액은 어느 정도입니까?

구 분	2018년도	2019년도	2020년도 (전망)
①전체 투자액(연구개발/건물/기계/설비 등)	백만원	백만원	백만원
②연구개발 투자액	백만원	백만원	백만원
③매출액 대비 연구개발투자 비율	%	%	%

3. 기술개발 시 애로사항은 무엇입니까? (복수선택 가능)

- ① 자금조달 ② 기술개발인력 확보 및 유지 ③ 기술 정보 부족 및 획득 곤란
④ 연구 설비기자재 부족 ⑤ 신기술의 짧은 수명주기 ⑥ 기타()

4. 귀사의 제품 매출액에 대한 아래의 비중은 어떻게 됩니까?

구 분	비중
자사제품 판매	%
국내 타사제품 유통	%
외산제품 유통	%
합 계	100%

* 제품 매출액의 합계는 2~3페이지의 정보보안 제품 매출액의 합계와 일치해야 합니다.

5. 귀사의 정보보안 관련 지적재산권 보유현황은? (2019년 7월 1일 기준)

구 분	지적재산권			
	특허권	실용신안권	의장권	상표권
현재 보유	건	건	건	건
현재 출원중	건	건	건	건

5-1. 귀사의 정보보안 관련 해외특허 보유현황은?(2019년 7월1일 기준)

해외특허권	현재 보유(건), 현재 출원중 (건)
-------	------------------------------------

6. 귀사가 중점을 두고 있는 주요 경쟁요소는 무엇입니까? (복수선택 가능)

※정보보안 시스템 개발 및 공급 기업만 해당

- ① 가격 ② 기술·품질 ③ 인지도 ④ 마케팅
⑤ 입지적 유리 ⑥ 기타 ()

7. 귀사는 경영 및 기술 관련 정보를 주로 어디에서 수집하십니까?

- ① 대학/연구소 ② 정부 및 공공기관 ③ 고객(납품모기업)
④ 제품/서비스 협력업 ⑤ 관련 업종단체/협회 ⑥ 컨설팅업체
⑦ 금융기관 ⑧ 종업체간 교류 ⑨ 기타 ()

8. 귀사의 정보보안 관련(제품/정보보호체계) 인증 보유 현황은?

① CC인증(건)
② GS인증(건)
③ ISO 27001 (건)
④ ISMS (건)
⑤ PIPL인증 (건)
⑥ CMVP인증 (건)
⑦ 기타(, 건)
⑧ 없음

9. 귀사는 해외지사 및 현지법인을 가지고 계십니까? ()

① 있다.
 (해외지사 지역: , , , ,)
 (현지법인 지역: , , , ,)

② 없다.

10. 귀사의 정보보안 사업 계약방식 비중(매출액기준)은 어떻게 되십니까?

구 분		공공사업	민간사업
공개입찰	협상에 의한 계약	%	%
	최저가낙찰	%	
수의계약		%	%
합계		100%	100%

10-1. 귀사의 사업에서 따른 직수주, 하도급 비율(매출액기준)은 어떻게 되십니까?

구 분	공공사업	민간사업
직수주 비율	%	%
하도급 비율	%	%
합계	100%	100%

11. (3페이지, 유지관리 매출액 발생 기업만)연간 유지관리(유지보수)의 효율은 어느 정도입니까?

구 분	공공사업	민간사업
유지관리 효율	%	%

※ “유지관리”라 함은 구매한 소프트웨어를 최적의 상태에서 활용/유지하기 위해 제공되는 제품지원, 기술 지원, 사용자지원 등의 서비스를 의미함

※ 유지관리 효율에 라이선스 갱신비용은 포함시키지 않음

11-1. (3페이지, 보안성지속서비스 매출액 발생 기업만)연간 보안성 지속 서비스의 효율은 어느 정도입니까?

구 분	공공사업	민간사업
보안성지속 서비스 효율	%	%

※ “보안성 지속 서비스”라 함은 정보보호제품을 활용하여 정보의 훼손, 변조, 유출 등을 방지하기 위해 지속적으로 요구되는 기술 기반의 서비스를 의미함

11-2. 연간 라이선스의 효율은 어느 정도입니까?

구 분	공공사업	민간사업
라이선스 효율	%	%

※ ‘라이선스 효율은 판매자가 구매자에게 제품, 지적재산권 사용을 허가해줄 때, 기준가격(출고가, 도매가 등)의 몇 %를 라이선스 비용으로 책정할 것인지를 의미함

VII. 정보보안 산업 시장경쟁 및 산업동향에 관한 질문입니다.

1. 다음은 귀 사의 주력 매출 분야에 대한 시장경쟁 상황과 산업동향에 관련된 문항입니다. 각 문항에 대해서 동의정도를 말씀해 주시기 바랍니다.

정보보안 산업분야(시장)		동의 정도 평가				
		전혀 그렇지 않다	별로 그렇지 않다	보통이다	다소 그렇다	매우 그렇다
성장성	1) 신기술, 신제품이 지속적으로 출현하고 있다	1	2	3	4	5
	2) 기업 이윤을 안정적으로 확보할 수 있다	1	2	3	4	5
	3) 기술 변화의 예측이 어느 정도 가능하다	1	2	3	4	5
경쟁성	4) 시장 규모가 포화상태이다	1	2	3	4	5
	5) 가격 경쟁이 치열하다	1	2	3	4	5
	6) 경쟁자 전략의 예측이 가능하다	1	2	3	4	5
	7) 신기술 습득을 위한 경쟁이 치열하다	1	2	3	4	5
기술력	8) 국산과 외산의 경쟁이 증가하고 있다	1	2	3	4	5
	9) 국내시장 기술력이 낮다	1	2	3	4	5
기타	10) 통합솔루션 제공이 미약하다	1	2	3	4	5
	11) 자금상황이 어려운 편이다	1	2	3	4	5

2. 정보보안산업 시장 확대를 위하여 정부지원이 필요한 부분은 무엇입니까?

- ① 전문인력 양성 ② 기술개발 지원 ③ 기술이전의 활성화
④ 법/제도 제·개정 ⑤ 공공부문의 시장수요 창출 ⑥ 소비촉진/투자활성화
⑦ 자금지원 및 세제혜택 ⑧ 해외지원 사업 확대 ⑨ 기타 ()

3. 해외진출 시 다음 항목에 대하여 애로사항은 어느 정도입니까?

구 분	매우 낮음	낮음	보통	높음	매우 높음
① 환율하락에 따른 채산성 악화	1	2	3	4	5
② 자금유동성부족	1	2	3	4	5
③ 현지 법 제도 및 관련정보	1	2	3	4	5
④ 판로개척	1	2	3	4	5
⑤ 관세·통관절차 부담	1	2	3	4	5
⑥ 지적재산권 보호역량 부족	1	2	3	4	5
⑦ 국제표준 및 인증획득	1	2	3	4	5
⑧ 세계경제 불안 및 경기둔화	1	2	3	4	5
⑨ 인력부족	1	2	3	4	5
⑩ 기타(직접 서술):					

☺ 장시간 정보보안 설문에 응답해 주셔서 대단히 감사합니다. ☺

□ 물리보안 기업용

I. 귀사의 일반현황에 관한 질문입니다.

회 사 명		설립년도	년	사업자등록번호			
대표이사 성명		대표이사 E-mail		종업원 수 (2018년 12월)	명	남자	명
소 재 지	①서울 ②부산 ③대구 ④인천 ⑤광주 ⑥대전 ⑦울산 ⑧경기 ⑨강원 ⑩충북 ⑪충남(세종) ⑫전북 ⑬전남 ⑭경북 ⑮경남 ⑯제주					여자	명
자본금	자본금: 백만원			보안인력 수 (2018년 12월)	명	남자	명
기업 형태	준거법 기준 1. 내국회사 2. 외국회사 자본구성 기준 1. 내자회사 2. 외자회사 3. 합작회사						여자
상 장 여 부	1. 비상장 2. 코스닥 3. 거래소 4. 코넥스			매출 현황	연간 총매출액	2018년	백만원
일반/벤처기업	1. 일반기업 2. 벤처기업					2019년(추정)	백만원
주사업 분야	1. 정보보호(정보보안/물리보안)사업이 주사업 2. 타사업이 주사업			물리보안 총매출액	2018년	백만원	
						2019년(추정)	백만원
주력제품/서비스	*첨부 '정보보호산업 분류표'를 참고하여 작성			2017년 수요처별 물리보안 매출비중(%)	공공/교육	금융기관	기업/기타

II. 귀사의 매출현황에 관한 질문입니다.

* 총계는 10페이지의 2018년, 2019년 물리보안 총매출액과 같아야 합니다.

※2019년 총매출은 상반기(6월말기준 실적액)와 하반기(7월이후 12월말기준 추정액) 합계

[단위: 백만원, %]

귀사에서 취급하는 물리보안 제품 또는 서비스를 분류표(첨부자료- 20 페이지 참고)에 따라 작성해주시고, 각각의 해당사항에 대해 숫자로 기입하여 주십시오.				총 매출액 (단위: 백만원)		
대분류	중분류	제품 및 서비스	2018년 매출액	2019년 매출액 (1월~6월)	2019년 매출액추정 (7월~12월)	
총 계 (S/N 물리보안+서비스)*						

1. 귀사는 4차산업관련 제품을 현재 개발 혹은 출시하고 있습니까? ()
 1) 있음, 이미 출시 2) 있음, 현재 개발 중임 3) 없음, 계획없음

1-1. 1)의 응답자의 경우, 현재 귀사에서 개발·활용하고 있는 4차 산업혁명 관련 기술 분야는 무엇입니까?

구분	관련 제품명	2018년 매출액 (단위: 백만원)	2019년 추정매출액 (단위: 백만원)
1.클라우드			
2.사물인터넷			
3.빅데이터			
4.인공지능			
5.블록체인			

2. 귀사의 2019년 매출은 작년과 비교하여 얼마나 악화 또는 호전이 예상되니까?

	악화가 예상된다 ----- 비슷하다 ----- 호전이 예상된다				
2019년 매출	①	②	③	④	⑤

- 2-1. 귀사의 2019년 매출이 작년 대비 악화 또는 호전이 예상되는 이유는 무엇입니까?

3. 귀사의 2020년 매출은 올해와 비교하여 얼마나 악화 또는 호전이 예상되니까?

	악화가 예상된다 ----- 비슷하다 ----- 호전이 예상된다				
2020년 매출	①	②	③	④	⑤

- 3-1. 귀사의 2020년 매출이 작년 대비 악화 또는 호전이 예상되는 이유는 무엇입니까?

III. 귀사의 수출 현황에 관한 질문입니다.

귀사에서 취급하는 물리보안 제품 또는 서비스를 각각의 해당사항에 대해 숫자로 기입하여 주십시오.

[단위: 백만원, %]

* 2018년 수출액은 상반기(6월말기준 실적액)와 하반기(7월이후 12월말기준 전망액)의 합계와 같아야 합니다.

귀사에서 취급하는 물리보안 제품 또는 서비스를 분류 표(첨부자료- 20페이지 참고)에 따라 작성해주시고, 각각의 해당사항에 대해 숫자로 기입하여 주십시오.			수 출							
			연도별 수출액 및 예상액 (단위: 백만원)			2018년 국가별 수출비중 (각 국가의 합 100%)				
대분류	중분류	제품 및 서비스	2018년 수출액	2019년 수출액 (1월~6월)	2019년 수출액추정 (7월~12월)	국가명(직접기입)				
						%	%	%	%	%
						%	%	%	%	%
						%	%	%	%	%
						%	%	%	%	%
						%	%	%	%	%
총 계 (S/N 물리보안+서비스)*										

1. 귀사에 해외로 진출하고 싶은 물리보안 제품 또는 서비스가 있다면, 무엇이고 진출하고 싶은 국가는 어디입니까?

대분류	중분류	소분류	희망 진출국가

2. 귀사의 2019년 수출은 작년과 비교하여 얼마나 악화 또는 호전이 예상됩니까?

	악화가 예상된다 ----- 비슷하다 ----- 호전이 예상된다				
2019년 수출	①	②	③	④	⑤

2-1. 귀사의 2019년 수출이 작년 대비 악화 또는 호전이 예상되는 이유는 무엇입니까?

()

3. 귀사의 2020년 수출은 올해와 비교하여 얼마나 악화 또는 호전이 예상됩니까?

	악화가 예상된다 ----- 비슷하다 ----- 호전이 예상된다				
2020년 수출	①	②	③	④	⑤

3-1. 귀사의 2020년 수출이 작년 대비 악화 또는 호전이 예상되는 이유는 무엇입니까?

()

IV. 귀사의 수입 현황에 관한 질문입니다.

1. 귀사에서는 물리보안 분야에서 2018년도나 2019년도에 해외로부터의 수입이 있었습니까?
① 있었음 => 2번으로 이동 ② 없었음 => V. 기술인력/고용 파트로 이동
2. 귀하가 2018년과 2019년에 수입하였거나 수입이 예상되는 금액, 수입국가를 간략하게 기술하여 주시기 바랍니다.

* 외국으로부터 직접 완제품이나 반제품을 구매한 것으로 응답기업체가 수입신고필증 상 수입자로 되어 있으며, 과세가격으로 표기된 금액

	2018년 수입액	2019년 상반기 수입액 (1월~6월)	2019년 하반기 수입액 (7월~12월)	2018년 수입국가
물리보안	백만원	백만원	백만원	

- * 외국으로부터 직접 완제품이나 반제품을 구매한 것으로 응답기업체가 수입신고필증 상 수입자로 되어있으며, 과세가격으로 표기된 금액

V. 귀사의 기술인력/고용 현황에 관한 질문입니다.

1. 귀사의 전체 종업원 수를 전공(최종학력 기준)으로 나누어 해당 칸에 기입하여 주십시오.(2018년 12월 말 기준)

구분	전공 학과	합계
1) 공과 계열(정보보안 제외)	전자 관련학과, 통신 관련학과, 컴퓨터 관련 학과, 기계/전기 관련학과 등	명
2) 정보보안(호)과	정보보안(호) 학과	명
3) 비관련학과	인문, 사회계열, 예·체능계열 등 정보통신 비관련학과 등	명
전체 합계(총 종업원 수)		명

- * 전체 합계는 13페이지 2018년 12월말 기준 총종업원 수와 같아야 합니다.

2. 2017년 12월말 기준, 귀사의 총 종업원 중 물리보안 관련 종사자를 수준별로 구분하여 기재하여 주십시오.

구 분	세부분류	세부 직종 예시	인원
제품 개발	Hardware	• PCB 및 전자 회로 등 제품의 Hardware 관련 개발	명
	응용 Software	• Window, Linux, RTOS 기반의 응용 Program 개발	명
영업	국내외 영업	• 국내외 고객을 대상으로 한 마케팅, 영업 기술 지원 등	명
기술지원	설계, 시공 및 감리	• SI营业을 위한 설계 및 제안서 작성 관련 업무 • 현장 감리 및 시공 관련 업무	명
생산	생산기술, 품질관리	• 생산 시스템 운영 전반에 관련 된 전문 업무 • 품질 관리 및 품질 시스템 운영에 필요한 업무	명
관리 및 기타	관리, 기타	• 내부 관리 업무·기타 명시되지 않은 업무	명
전체 합계(총 보안 인력)			명

- * 2018년 12월말 기준 물리보안 인력의 전체합계는 13페이지의 해당년도 총 보안인력 수와 같아야 합니다.

3. 2018년 12월말 기준, 귀사의 총 종업원 중 정보보안 관련 기술 및 연구인력 종사자를 경력으로 구분하여 해당 칸에 기재하여 주십시오.

설명	인원
물리보안 관련 경력 4년 미만	명
물리보안 관련 경력 4년 이상 7년 미만	명
물리보안 관련 경력 7년 이상 11년 미만	명
물리보안 관련 경력 11년 이상 15년 미만	명
물리보안 관련 경력 15년 이상	명
전체 합계(총 보안 인력)	명

* 2018년 12월 기준 정보보안 인력의 전체합계는 2페이지의 해당년도 총 보안인력 수와 같아야 합니다.

4. 귀사에서는 물리보안 관련 인력을 채용했거나 채용할 계획이 있습니까?(채용하지 않았거나 계획이 없는 경우, '0'으로 표시)

구분	2019년 (상반기 채용 및 하반기 예상)	2020년 (채용 계획)
신입	명	명
경력	명	명
합계	명	명

VI. 귀사의 기술/연구개발 및 기업 경쟁력 관련 질문입니다.

1. 귀사는 기술개발 관련 자체기술연구소나 전담부서를 운영하고 있습니까?

① 기업부설연구소 운영(명) ② 연구개발전담부서 운영(명) ③ 없음

2. 귀사의 물리보안산업 관련 전체 투자액 및 연구개발 관련 투자액은 어느 정도 입니까?

구분	2018년도	2019년도	2020년도(전망)
①전체 투자액(연구개발/건물/기계/설비 등)	백만원	백만원	백만원
②연구개발 투자액	백만원	백만원	백만원
③매출액 대비 연구개발투자 비율	%	%	%

3. 기술개발 시 애로사항은 무엇입니까? (복수선택 가능)

① 자금조달 ② 기술개발인력 확보 및 유지 ③ 기술 정보 부족 및 획득 곤란
④ 연구 설비기자재 부족 ⑤ 신기술의 짧은 수명주기 ⑥ 기타()

4. 귀사의 제품 매출액에 대한 아래의 비중은 어떻게 됩니까?

구 분	비중
자사제품 판매	%
국내 타사제품 유통	%
외산제품 유통	%
합 계	100%

* 제품 매출액의 합계는 2~3페이지의 정보보안 제품 매출액의 합계와 일치해야 합니다.

5. 귀사의 물리보안 관련 지적재산권 보유현황은? (2019년 7월 1일 기준)

구 분	지적재산권			
	특허권	실용신안권	의장권	상표권
현재 보유	건	건	건	건
현재 출원중	건	건	건	건

5-1. 귀사의 정보보안 관련 해외특허 보유현황은?(2019년 7월1일 기준)

해외특허권	현재 보유(건), 현재 출원중 (건)
-------	--

6. 귀사가 중점을 두고 있는 주요 경쟁요소는 무엇입니까? (복수선택 가능)

- ① 가격 ② 기술·품질 ③ 인지도
④ 마케팅 ⑤ 입지적 유리 ⑥ 기타 ()

7. 귀사는 경영 및 기술 관련 정보를 주로 어디에서 수집하십니까? (복수선택 가능)

- ① 대학/연구소 ② 정부 및 공공기관 ③ 고객(납품모기업)
- ④ 제품/서비스 협력업체 ⑤ 관련 업종단체/협회 ⑥ 컨설팅업체
- ⑦ 금융기관 ⑧ 종업채간 교류 ⑨ 기타 ()

8. 귀사의 물리보안 관련(제품/정보보호체계) 인증 보유 현황은?

① KC 인증(건)
② 해외 인증(인증명: , 건)
③ 해외 인증(인증명: , 건)
④ 해외 인증(인증명: , 건)
⑤ 기타(, 건)

9. 귀사는 해외지사 및 현지법인을 가지고 계십니까? ()

- ① 있다.
- | | | | | | | | | | | |
|-----------|--|---|--|---|--|---|--|---|--|---|
| (해외지사 지역: | | , | | , | | , | | , | |) |
| (현지법인 지역: | | , | | , | | , | | , | |) |
- ② 없다.

10. 귀사의 물리보안 사업 계약방식 비중(매출액기준)은 어떻게 되십니까?

구 분		공공사업	민간사업
공개입찰	협상에 의한 계약	%	%
	최저가낙찰	%	
수계약		%	%
합계		100%	100%

10-1. 귀사의 사업에서 따른 직수주, 하도급 비율(매출액기준)은 어떻게 되십니까?

구 분	공공사업	민간사업
직수주 비율	%	%
하도급 비율	%	%
합계	100%	100%

VII. 물리보안 산업 시장경쟁 및 산업동향에 관한 질문입니다.

1. 다음은 귀사의 주력 매출 분야에 대한 시장경쟁 상황과 산업동향에 관련된 문항입니다. 각 문항에 대해서 동의정도를 말씀해 주시기 바랍니다.

정보보안 산업분야(시장)		동의 정도 평가				
		전혀 그렇지 않다	별로 그렇지 않다	보통이다	다소 그렇다	매우 그렇다
성장성	1) 신기술, 신제품이 지속적으로 출현하고 있다	1	2	3	4	5
	2) 기업 이윤을 안정적으로 확보할 수 있다	1	2	3	4	5
	3) 기술 변화의 예측이 어느 정도 가능하다	1	2	3	4	5
경쟁성	4) 시장 규모가 포화상태이다	1	2	3	4	5
	5) 가격 경쟁이 치열하다	1	2	3	4	5
	6) 경쟁자 전략의 예측이 가능하다	1	2	3	4	5
	7) 신기술 습득을 위한 경쟁이 치열하다	1	2	3	4	5
	8) 국산과 외산의 경쟁이 증가하고 있다	1	2	3	4	5
기술력	9) 국내시장 기술력이 낮다	1	2	3	4	5
	10) 통합솔루션 제공이 미약하다	1	2	3	4	5
기타	11) 자금상황이 어려운 편이다	1	2	3	4	5

2. 물리보안산업 시장 확대를 위하여 정부지원이 필요한 부분은 무엇입니까?

- | | | |
|---------------|-----------------|--------------|
| ① 전문인력 양성 | ② 기술개발 지원 | ③ 기술이전의 활성화 |
| ④ 법/제도 제·개정 | ⑤ 공공부문의 시장수요 창출 | ⑥ 소비촉진/투자활성화 |
| ⑦ 자금지원 및 세제혜택 | ⑧ 해외지원 사업 확대 | ⑨ 기타 () |

3. 해외진출 시 다음 항목에 대하여 애로사항은 어느 정도입니까?

구 분	매우 낮음	낮음	보통	높음	매우 높음
① 환율하락에 따른 채산성 악화	1	2	3	4	5
② 자금유동성부족	1	2	3	4	5
③ 현지 법 제도 및 관련정보	1	2	3	4	5
④ 판로개척	1	2	3	4	5
⑤ 관세·통관절차 부담	1	2	3	4	5
⑥ 지적재산권 보호역량 부족	1	2	3	4	5
⑦ 국제표준 및 인증획득	1	2	3	4	5
⑧ 세계경제 불안 및 경기둔화	1	2	3	4	5
⑨ 인력부족	1	2	3	4	5
⑩ 기타(직접 서술):					

☺ 장시간 물리보안 설문에 응답해 주셔서 대단히 감사합니다. ☺

부록3

1-1. 정보보안 기업 매출현황 통계

구분		2018년	2019년	증감율(%)
정보보안 시스템 개발 및 공급	네트워크보안 시스템 개발	729,393	771,656	5.8
	시스템보안 솔루션 개발	488,402	523,115	7.1
	정보유출방지 시스템 개발	426,128	456,251	7.1
	암호/인증 시스템 개발	151,879	161,760	6.5
	보안관리 시스템 개발	297,920	327,790	10.0
	소계	2,093,723	2,240,572	7.0
정보보안 관련 서비스	보안컨설팅 서비스	302,099	321,478	6.4
	보안시스템유지관리/ 보안성 지속 서비스	351,942	359,645	2.2
	보안관제 서비스	273,927	286,880	4.7
	보안교육 및 훈련 서비스	1,740	2,990	71.8
	공인/사설 인증서	59,496	66,122	11.1
	소계	989,203	1,037,115	4.8
합계		3,082,926	3,277,687	6.3

1-2. 정보보안 기업 수출현황 통계

구분		총수출액(백만원)		2018년 국가별 수출 비중				
대분류	중분류	2018년	2019년(E)	일본	중국	미국	유럽	기타
정보보안 시스템 개발 및 공급	네트워크보안 시스템 개발	27,642	33,574	45.5	8.4	9.6	1.4	35.1
	시스템보안 솔루션 개발	15,319	14,814	41.4	21.5	3.7	1.2	32.2
	정보유출방지 시스템 개발	9,926	12,324	55.2	14.7	2.9	0	27.2
	암호/인증 시스템 개발	3,032	3,108	48.2	24.5	2.5	0	24.8
	보안관리 시스템 개발	7,024	7,159	40.2	21.1	11.1	2.9	24.7
	합계	62,943	70,979	45.6	14.8	6.9	1.2	31.5
정보보안 관련 서비스	보안컨설팅 서비스	5,934	22,017	32.0	63.8	0	0	4.2
	보안시스템 유지관리/ 보안성 지속서비스	9,594	10,054	70.6	22.4	1.6	0.7	4.7
	보안관제 서비스	3,892	5,478	82.2	0	1.7	0	16.1
	합계	19,420	37,549	61.1	30.6	1.1	0.3	6.8
총계		82,363	108,528	49.2	18.5	5.6	1.0	25.7

1-3. 정보보안 기업 인력/고용 통계

구분	세부 분류	4년 미만	4년 이상 7년 미만	7년 이상 11년 미만	11년 이상 15년 미만	15년 이상	합계 (명)	비중 (%)
정보보안 연구 및 개발직	암호 및 인증 기술, 시스템 및 네트워크 기술, 응용기술 및 서비스	1,877	1,197	793	451	279	4,597	34.4
정보보안 관리직	정보시스템 관리	626	1,017	692	322	125	2,782	20.8
	정보보안 컨설팅	336	665	431	187	77	1,696	12.7
	정보보안 관제	542	588	505	239	57	1,931	14.4
정보보안 영업직	정보보안 마케팅	367	382	423	519	242	1,933	14.4
기타 정보보안 관련직	정보시스템 감리 및 인증, 정보보안 교육, 기타	89	59	71	107	113	439	3.3
합 계		3,837	3,908	2,915	1,825	893	13,378	100.0

구분	2019년(상반기 기재용 및 하반기 예상 채용인력 포함)		2020년(계획)	
채용직(명)	신입	경력	신입	경력
	803	1,003	625	709

2-1. 물리보안 기업 매출현황 통계

구분		2018년	2019년(E)	증감율(%)
물리보안 시스템 개발 및 공급	보안용 카메라 제조	1,106,250	1,171,005	5.9
	보안용 저장장치 제조	907,487	923,263	1.7
	CCTV 카메라 부품	484,766	506,379	4.5
	물리보안 솔루션	378,902	419,198	10.6
	물리보안 주변장비	161,576	164,153	1.6
	출입통제 장비 제조	499,455	505,019	1.1
	생체인식 보안시스템 제조	293,378	315,218	7.4
	경보/감시 장비 제조	220,715	221,179	0.2
	기타 제품	369,398	374,307	1.3
	소계	4,421,927	4,599,723	4.0
물리보안 관련 서비스	출동보안서비스	1,726,210	1,727,972	0.1
	영상보안서비스	401,777	415,647	3.5
	기타보안서비스	485,004	536,208	10.6
	소계	2,612,991	2,679,827	2.6
합계		7,034,918	7,279,550	3.5

2-2. 물리보안 기업 수출현황 통계

구분		총수출액(백만원)		2018년 국가별 수출 비중(%)				
대분류	중분류	2018년	2019년(E)	일본	중국	미국	유럽	기타
물리보안 시스템 개발 및 공급	보안용 카메라 제조	516,223	541,936	14.9	7.6	17.1	18.7	41.7
	보안용 저장장치 제조	441,229	457,908	13.5	5.2	21.5	16.1	43.7
	CCTV 카메라 부품	174,426	182,749	10.6	22.5	14.2	8.9	43.8
	물리보안 솔루션	106,278	110,988	5.5	2.3	24.4	15.9	51.9
	물리보안 주변장비	23,281	22,424	16.8	5.7	60.3	17.2	0
	출입통제 장비 제조	89,732	96,808	11.2	19.6	10.2	14.6	44.4
	생체인식 보안시스템 제조	22,281	24,203	5.2	0	18.8	18.8	57.2
	경보/감시 장비 제조	469	582	5.2	32.8	5.3	0	56.7
	기타 제품	99,637	99,864	10.2	3.1	15.9	18.9	51.9
	합계	1,473,556	1,537,462	12.6	8.6	18.8	16.3	43.7
물리보안 관련 서비스	기타보안서비스	213	323	0	0	0	10.0	90.0
총계		1,473,769	1,537,785	12.6	8.6	18.8	16.3	43.7

2-3. 물리보안 기업 인력/고용 통계

1. 2017년 12월 기준 귀사의 총 종업원 중 물리보안 관련 종사자를 수준별로 구분하여 해당 칸에 기재하여 주십시오.

구분	세부 분류	4년 미만	4년 이상 7년 미만	7년 이상 11년 미만	11년 이상 15년 미만	15년 이상	합계(명)	비중(%)
제품 개발	Hardware	1,821	1,478	1,389	1,248	506	6,442	19.6
	응용 Software	1,200	1,279	1,304	643	344	4,770	14.5
영업	국내외 영업	1,108	1,075	1,400	820	509	4,912	14.9
기술 지원	설계, 시공 및 감리	732	1,097	1,064	587	443	3,923	11.9
생산	생산 기술, 품질 관리	1,194	949	1,177	771	456	4,547	13.8
관리 및 기타	관리, 기타	3,856	2,548	1,189	374	336	8,303	25.2
합계		9,911	8,426	7,523	4,443	2,594	32,897	100.0

구분	2019년(상반기 기재용 및 하반기 예상 채용인력 포함)		2020년(계획)	
채용직(명)	신입	경력	신입	경력
	1,166	1,686	1,131	1,656



별첨

1	인공지능 기반의 보안기술 동향 및 고려사항	189
2	양자암호통신과 보안의 미래	204
3	5G 시대의 위협과 보안	215
4	융합보안의 현황과 미래전망	225
5	얼굴인식시스템 동향 및 전망	237



인공지능 기반의 보안기술 동향 및 고려사항

이글루시큐리티, 정일옥 부장

1. 인공지능 기반 보안 필요성

다양한 분야에서 지능화·고도화되어 가는 사이버위협 증가

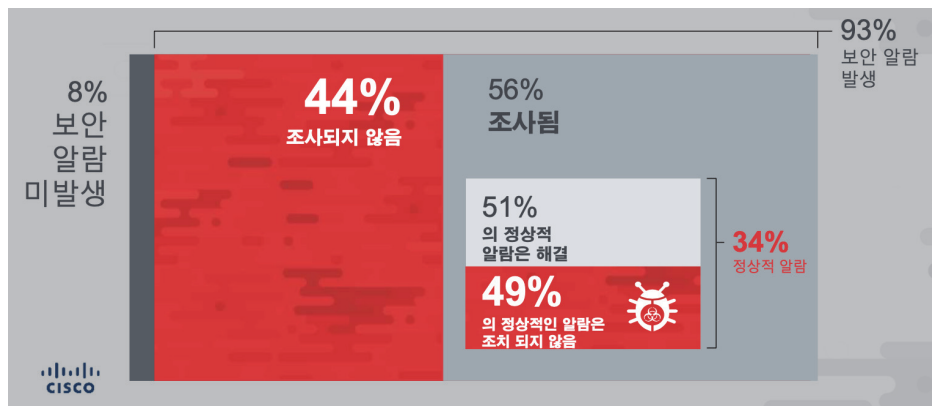
새로운 ICT 환경에서 사이버위협은 복합적인 공격기법을 사용한 신·변종 위협의 증가와 함께 고도화되고 있으며 국내외에서 다양한 위협사례 발생하고 있다. 국내의 경우 2018년 암호화폐 채굴장 정보탈취 공격, 평창올림픽 해킹사고, 쇼핑몰 웹 어플리케이션 취약점 공격 등 사이버위협이 심각해지고 있으며, 해외에서도 제조, 의료, 교통 등 다양한 분야에서 ICT 기술과 융합 발전하면서 사이버공격 사례가 전 분야에서 발생하고 있다.

사이버보안 위협의 증가에 대응할 수 있는 사이버 보안역량이 한계에 직면

이러한 상황에서 전 세계적인 사이버보안 인력의 부족 등으로 인해 기업, 기관들은 점점 증가하는 사이버위협에 효과적으로 대처하는 데 어려움을 겪고 있다. 기업들은 사이버위기에 직면한 상황에서 최근 기계학습, 딥러닝 등의 발전에 따른 인공지능(AI)의 잠재력을 이용하여 인력난을 해결할 수 있다고 기대하고 있다.

국내에서도 주요부처에서 운영하는 전산장비 수가 매년 평균 5% 규모로 증가하고 있으나, 운영 인력과 투자는 정체 상태에 있다. 대부분의 주요 부처들이 사이버안전센터에서 빅데이터 기반의 보안체계를 구축 완료하여 대량의 로그를 수집하고 있으며, 이를 통해 관제 직원의 대응처리에 한계가 발생하고 있다. 글로벌 보안업체인 시스코(CISCO)에 따르면, 사이버보안 침입을 알리는 경보의 44%는 조사되지 않고, 조사된 56% 경보 중 불과 약 3분의 1(34%)이 대응조치가 필요한 것으로 파악되나, 이 중 조치되는 비율은 51%이고, 나머지 49%는 미해결 상태로 남겨있어 이에 대한 해결책이 필요하다고 말하고 있다.

[그림] 보안위협 정보의 경고알람 및 대응처리 현황

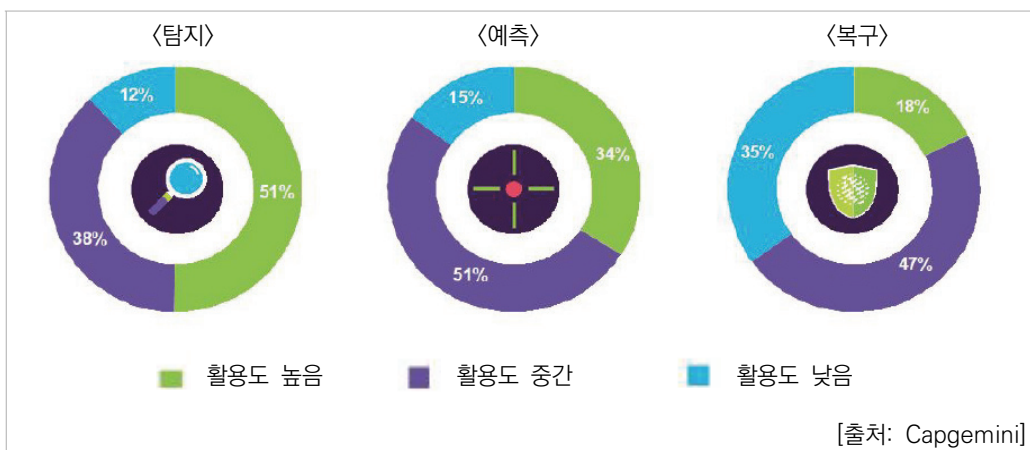


[출처: Cisco, 2019 연례 사이버보안 보고서]

네트워크 보안역량의 한계, 데이터 급증, IoT 등 기술연계로 인한 기하급수적 기기, 센서 등의 확대로 다양한 사이버보안 분야에서 AI 적용에 관심

기업들의 AI 활용분야는 주로 네트워크 보안에 집중되어 있고, 데이터 경제 부상 등으로 데이터 보안에 대한 AI 활용에도 관심이 증가하면서 기업들은 사이버위협의 탐지, 예측, 대응에 광범위하게 인공지능을 적용하고 있고, 특히 탐지 영역에서 인공지능 활용에 예산과 시간을 투자하는 경향이 있으며, 향후 기업이 사이버보안 효율성 개선을 위해 인공지능을 채택함에 따라 기계학습 기술이 발전하면서 예측과 복구 분야도 점진적으로 증가할 것으로 예상하고 있다.

[그림] 사이버보안 영역(탐지, 예측, 복구)별 AI 활용 비율



[출처: Capgemini]

보안전문 조사기관인 포네몬(Ponemon) 발간 보고서에 따르면 보안에 인공지능을 적용한 경우 위협분석 시간 단축(69%), 외부 바이러스 감염요소 억제(64%), 애플리케이션의 보안 취약점 식별(60%) 등 기업의 업무 효율성이 향상되는 것으로 조사하고 있으며, 보안기술에 인공지능을 적용한 기업의 사이버위협 대응비용은 연평균 80만 달러, 그렇지 않은 기업은 연평균 330만 달러 이상 지출되어, 연 2백만 달러 이상 절감할 것으로 보고 있다.

[표] AI 적용 전·후의 사이버대응 소요시간 비교

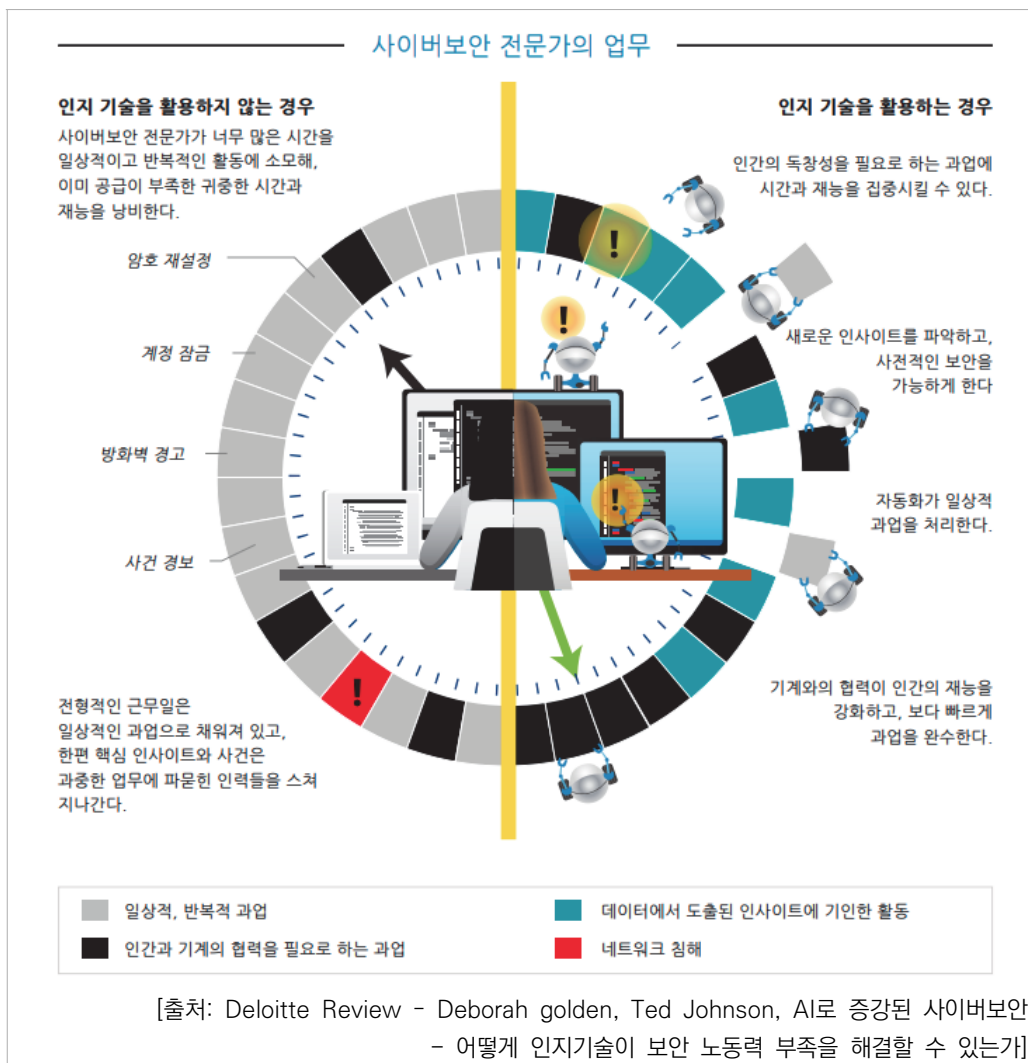
* \$62.50/시간

구분	AI 적용 전	AI 적용 후	시간/비용 차이
사이버방어 조직 및 계획	25.32	16.05	9.27
사이버침해 및 말웨어 감염의 실행가능한 정보 포착	80.20	41.11	39.09
애플리케이션 취약점 조사, 탐지	195.88	70.48	125.40
사이버침해나 말웨어에 대한 실행가능한 정보 조사	66.28	24.23	42.05
사이버침해나 말웨어로 인해 손상되거나 침해된 네트워크, 애플리케이션, 디바이스 치료	212.89	39.63	173.26
정책이나 의무사항을 준수하여 사이버사고에 대한 보고서 작성, 보고	25.07	15.91	9.16
오류, 긍정 오류의 추적에 보안인력이 소모하는 시간	400.83	41.42	359.41
말웨어 감염 네트워크, 애플리케이션, 디바이스 조치에 따른 계획에 없던 시스템 중단	3.95	1.90	2.05
주별 전체 시간	1,010.42	250.73	759.69
연간 전체 시간	52,541.84	13,037.96	39,503.88
연간 전체 비용 추정치	\$3,283,865.00	\$814,872.50	\$2,468,992.50*

[출처: Ponemon Institute(2018), The value of AI in Cybersecurity]

또한, 딜로이트에서는 사이버 보안의 인공지능 적용은 보안업무 종사자의 일상적·반복적 과업을 줄이고, 좀 더 고도화되고 전문적인 업무에 집중할 수 있도록 할 것으로 기대하고 있다.

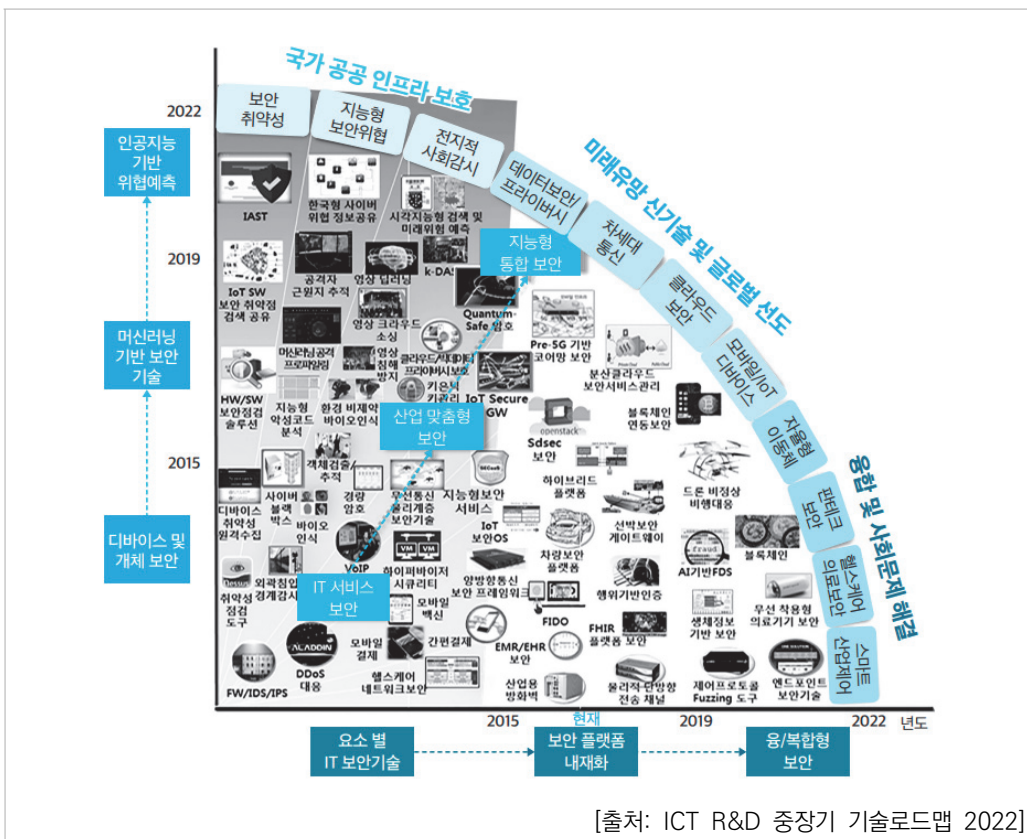
[그림] 사이버보안 전문가의 업무



2. 인공지능 기반의 보안기술 현황

최근 정보보호 기술은 기존의 디바이스 및 개체보안에 머신러닝 기반의 보안기술을 적용하고 있으며, 이는 향후 인공지능 기반의 위협예측으로 변하고 있다.

[그림] 정보보호 기술 발전 전망



[출처: ICT R&D 중장기 기술로드맵 2022]

또한, 사이버공격에 대한 방어 체계는 그동안 단계적으로 변화를 거쳐 왔다. 단위 보안장비에 의해 경계부분을 집중으로 방어하는 주변통제 기반의 제한된 보안과 방대한 데이터를 기반으로 하는 취약점 탐지, 최근에는 이해하고 추론하여 학습하는 보안으로 변하고 있다.

또한, 최근의 보안 트렌드를 살펴보면 민간 영역에서 발생하는 위협의 범위가 국가 안보를 위협하는 수준으로 확대될 뿐만 아니라, 정보유출에 국한되던 공격의 강도가 인간의 생명을 위협하는 수준으로 높아지고 있으며, 이렇게 보안 위협의 범위와 강도가 증가하는 원인은 4차 산업혁명을 주도하는 신기술의 급속한 발전에 따른 것이다.

이를 통해, 다양한 보안영역에 인공지능 기술을 적용하고 있으며, 이를 활용한 보안 시스템 및 서비스 증가하고 있다. 인공지능 기반 적응형 보안관제시스템은 단순 보안 관제 영역을 인공지능으로 대체, 기존의 보안관제 인력의 실용적 배치, 인공지능 보안 모델 적용의 선순환 체계 마련하는데 있으며, 침입탐지 및 예방 영역에서는 전 세계 위협 정보를 수집하여 새로운 위협 사전 탐지 및 예방을 통해 알려진 위협에만 대응하는 Signature 기반의 한계를 극복하여 새로운 위협 예방하는데 있다. 침해사고 후 진단 및 대응영역에서는 침해사고 원인을 AI가 진단하고 이에 맞는 조치 방법 제안하고, 침투 테스트에서는 화이트 해커에 의존하던 침투테스트를 인공지능을 통해 침투를 지원·대처함으로써 보다 견고한 보안취약점 개선을 보장하려 한다.

3. 보안 분야별 인공지능 기반의 적용기술

그 중 인공지능 기반의 보안기술은 Event Correlation, Threat Detection, Network Anomaly Detection 등 다양하며, 이를 ML, DL 등 다양한 인공지능 기술과 알고리즘을 통해 구현하고 있다.

[표] 인공지능 기반의 보안기술

보안기술	인공지능 기술	알고리즘
Event Correlation	Long-term Correlation Analysis	TF-IDF, Data Mining
Threat Detection	신경망 기반 침해위협 분석	K-NN, Neural Network
Network Anomaly Detection	ML 기반 Network Anomaly Detection	Semi-Supervised Learning
Host/Application Anomaly Detection	DL 기반 Malware Detection	Convolutional NN
User Behavior Analytics	AI 기반 User Behavior Analytics	

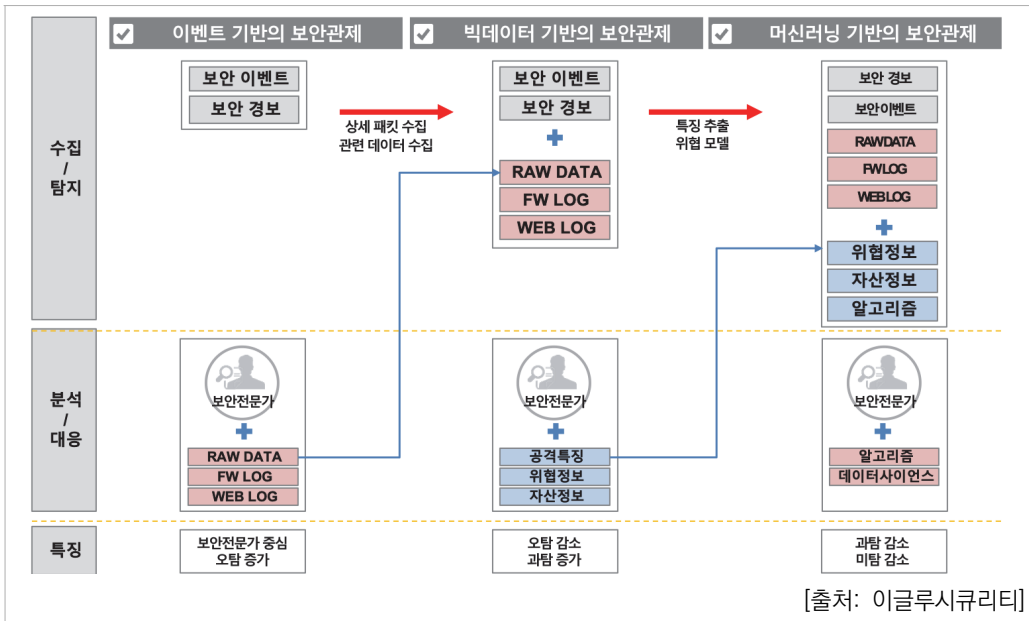
[출처 : 네트워크 보안에서의 인공지능 활용 ETRI]

이를 통해 보안 분야별로 인공지능 기반의 적용기술을 적용하는데 그중 가장 활발한 사례 중 보안관제, 네트워크, 악성코드 분야를 살펴보도록 한다.

보안관제 분야

현 보안관제는 지속적으로 진화해 왔으며, 한정된 시간과 가용 자원으로 기하급수적으로 증가하고 있는 방대한 데이터를 정확하고 신속하게 분석할 수 있는 인공지능을 통합보안관제에 적용하려는 노력이 활발하게 진행되고 있다.

[그림] 기존 보안관제체계와의 비교



보안관제에서의 수집대상은 지도 학습의 경우 IPS, WAF, SIEM 경고 등 보안관제요원이 직접 보고 판단할 수 있는 보안이벤트와 비지도 학습의 경우 FW, WEB log, Netflow, 시스템 로그 등으로 보안관제요원이 사고분석 시 사용되는 로그 등이 사용된다. 최근 구축 사례를 보면 보안관제에서는 수집대상으로 빅데이터 기반의 보안관제시스템을 수집 시스템의 연계대상으로 선택하는 경우가 많이 있다.

보안관제에 적용된 인공지능 기반의 기술은 지도와 비지도 학습으로 나눌 수 있으며, 지도 학습에 의한 보안이벤트 정·오탐 식별과 비지도 학습에 의한 이상행위 탐지로 나눌 수 있다.

보안관제에 인공지능을 적용한 전문업체로는 국내 기업 중에서는 기존의 빅데이터 기반의 보안관제시스템에서 인공지능 기반의 보안관제시스템의 도약을 준비하여 솔루션으로 출시된 곳도 있으며, 글로벌 제품을 통해 보안관제서비스에 인공지능을 도입한 곳도 있다. 대표적으로 통합보안관리시스템(ESM)으로 국내 보안관제시스템 시장을 개척했고 보안관제 서비스 시장에서 상당한 점유율을 확보, 유지하고 있는 이글루시큐리티(www.igloosec.com)는 최초로 인공지능을 접목한 대구시의 “지능형 보안관제시스템 (D-Security) 구축사업”을 완료하였으며, 수많은 보안 이벤트 분석 한계를 인공지능으로 해결하고 실시간 위협에 대한 대응력을 강화하는 것을 목표로 국내 최초 AI 보안관제 솔루션인 “SPiDER TM AI Edition”을 2019년 2월에 출시하여 다양한 공공기관에 구축하고 있음. 시큐아이는 자사의 보안관제센터에 IBM의 인공지능 기반 보안

분석기술인 “왓슨 포 사이버시큐리티(Watson for Cyber Security)”를 적용한 원격보안 관제센터를 구축하여 운영 중에 있다.

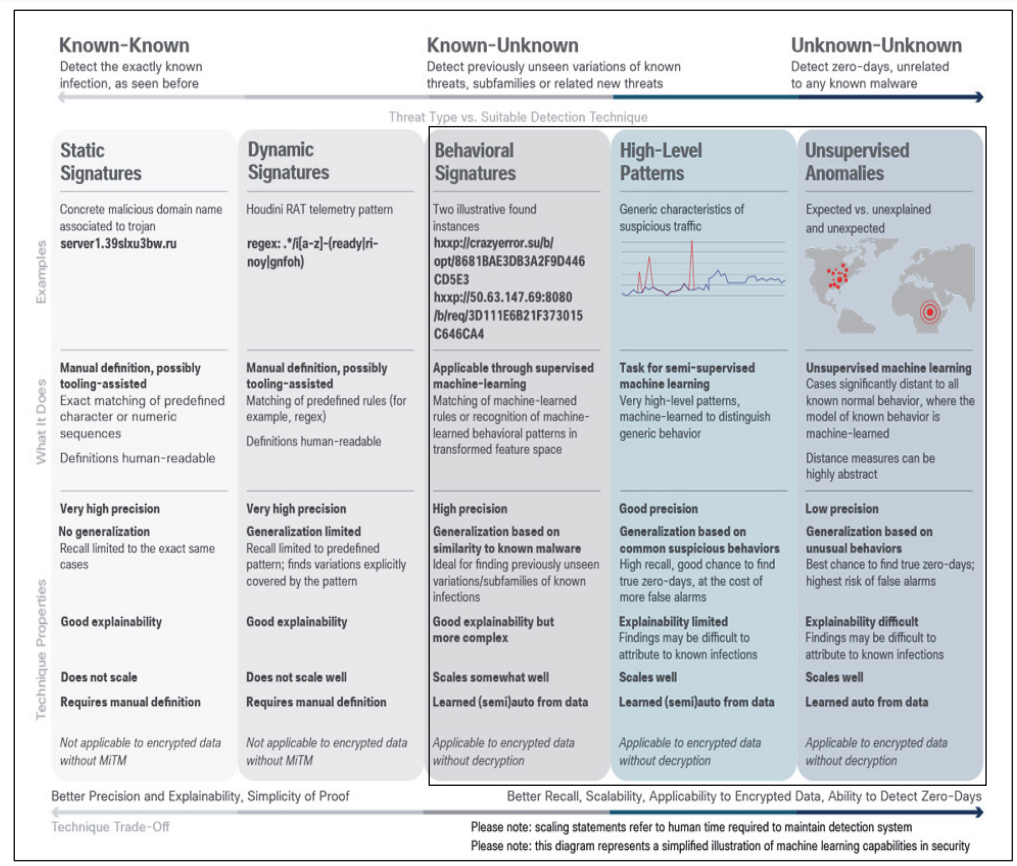
보안관제에 인공지능을 도입함으로써 인해 현 관제체계의 문제점 해결 시도를 하고 있으며, 이를 통해 관제인력 상향표준화 및 분석시간 단축 등의 효과를 볼 수 있다.

- 보안이벤트 정·오탐 예측을 통한 경보이벤트에 대한 분석시간 단축
- 이상행위 탐지를 통한 기존의 보안장비에서 탐지되지 않던 위협의 최소화
- 한정된 시간과 가용 자원으로 기하급수적으로 증가하고 있는 방대한 데이터를 정확하고 신속하게 분석 가능
- 인력 교체·업무의 피로감 등으로 인해 관제 수준이 주관적일 수 있는데 인공지능을 통해 관제인력 상향 표준화

네트워크 보안 분야

현재 사용되는 대부분의 네트워크 보안 상용제품은 시그니처 및 룰 기반의 시나리오에 기반 하여 공격을 탐지·차단하고 있다. 이러한 방식은 비교적 높은 정확도를 보여주며, 어느 정도 효율성이 있으나 각종 공격을 분석하고 패턴을 만드는데 전문성과 유지보수 비용이 발생하고 있다. 또한, 기존의 패턴을 우회하거나 변형된 공격을 감지하기에는 어려운 단점이 있다. 정상적인 네트워크 사용자들에 대한 통계자료를 만들어 놓고 그 범위를 벗어나면 침입이 발생했다고 하는 통계적 기반의 비정상 행위 탐지(Statistics-Based Anomaly Detection) 기법도 사용되고 있으나, 네트워크에서 발생하는 모든 행위로부터 위협을 식별하고 실시간으로 관리하기에는 한계가 있다.

[그림] 네트워크 보안에서의 머신러닝 분류체계



적용기술로는 지도학습을 통한 공통적인 기본위협에 대한 탐지 기술과 비지도 학습에 의한 내부 사용자 이상행위 탐지 등이 있다.

네트워크 탐지 분야에서 인공지능을 적용한 제품으로는 다크트레이스(DarkTrace), Vectra 등이 있으며, 다크트레이스는 비지도 학습기반의 머신러닝 기법을 활용하며 인간의 면역체계와 유사하게 제작되어 단말, 서버 등 모든 디바이스에 대한 데이터 흐름을 통해서 정상행위를 학습하고 이에 반하는 이상행위를 판별. 또한, 수학적 모델링에 근간하고, 시그니처와 톨에 의존하지 않기에 지속적으로 발생하는 지능적이고 고도화된 공격에 대한 대처가 가능하다고 한다. Vectra의 위협탐지 접근방법은 데이터사이언스 및 머신러닝을 기반으로 인간의 전문적인 지식과 조화를 추구하고, 위협탐지 알고리즘은 위협 정보의 연속 사이클을 분석하면서 지도 학습과 비지도 학습을 지속적으로 병행하여 위협모델을 탐지하는 방식이다.

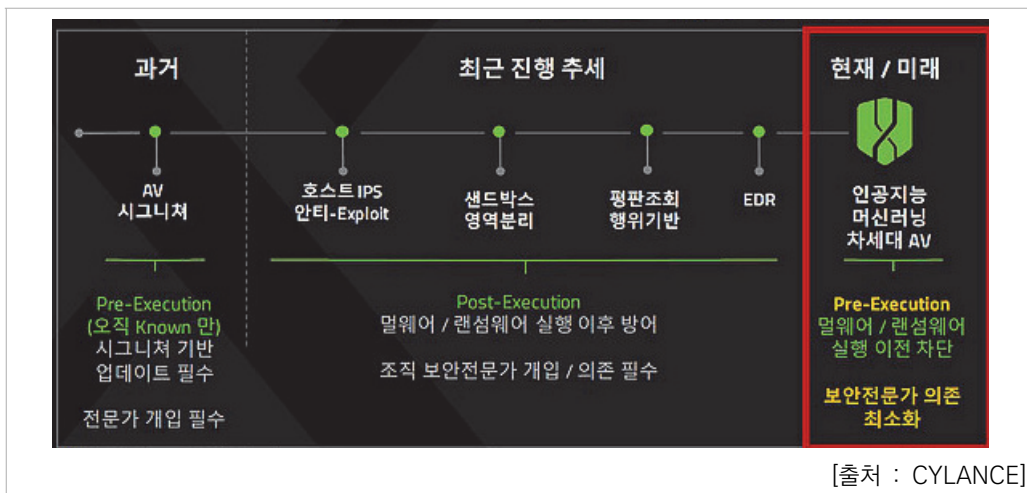
기대효과는 머신러닝과 인공지능 알고리즘을 기반으로 네트워크상의 모든 디바이스 및 사용자 고유의 '행위 패턴'을 반복적으로 파악하고, 기존의 방식으로 탐지하기 어려

운 새로운 위협에 대한 식별이 가능하다. 특히, 사전 지식이나 사용자 인증 없이 자동으로 동작하며, 네트워크 내에서 탐지하기 어려운 은밀한 공격을 실시간으로 탐지하고 차단 가능하다.

악성코드 분야

기존 시그니처 백신은 기존에 수집된 악성코드의 샘플 또는 패턴을 분석 및 진단하여 치료 방법을 알아내고 이를 안티 바이러스 데이터베이스에 추가하는 방식으로, 데이터베이스에 추가된 악성코드 공격이 다시 발생할 경우 신속한 대응이 가능하나, 저장되어 있지 않은 공격에 대해서는 대응 방안이 미흡하여 이를 해결하기 위한 방법은 새로운 악성 코드를 빠르게 분석하여 데이터베이스에 업데이트하는 것이며, 인간보다는 인공지능이 2~10배 빠르게 진행할 수 있기 때문에 이를 적용한다.

[그림] 악성코드 분석에 대한 흐름도



관련 적용 기술로는 딥러닝 기반의 악성파일 탐지 기술, 악성코드 유사도 측정 기술 등을 적용하고 있다.

관련 기업으로는 기존 백신에 인공지능 기반의 엔진을 탑재하는 백신과 사용자 PC에 대한 실시간 탐지 및 분석을 통해 대응 하는 EDR(Endpoint Detection and Response) 솔루션이 급부상하고 있다. 블랙베리 사일런스는 프로세스 신규 생성 또는 라이브러리 로딩 시 해당 파일을 검사하여 악성일 경우에만 실행 전 차단하며, 기존의 신종, 변종 악성코드, 랜섬웨어 등의 실시간 사전 차단이 가능한 EDR 솔루션을 내놓았으며, 트렌드마이크로는 자사 “클라우드 앱 시큐리티(Cloud App Security)”에 인공지능 기술을 접목하여 위협 감지 기능을 강화하고, 세인트시큐리티는 인공지능 기반

안티바이러스 ‘MAX’를, 기존의 백신 강가인 안랩, 이스트시큐리티에서는 백신에 인공지능 엔진 탑재하고 있다.

4. 향후 인공지능 보안기술에 대두될 이슈 및 고려사항

최근 인공지능 기반의 보안기술을 적용한 시도가 증가하면서 현재는 적용을 위한 초기 단계이기 때문에 정확성과 성능에 대한 부분이 주요 이슈이지만, 향후 다양한 부분에서 고려해야 할 사항이 있다.

인공지능 보안기술에 발생 가능한 이슈

첫째, 사이버위협에 대한 대응력을 강화하기 위해서는 보안시스템간의 위협 정보에 대한 연계표준화 필요하다. 현재는 인공지능 기반의 보안시스템이 고도화 되고 정확성이 증가하면서 기존에 운영 중인 보안시스템과의 연계 중요성이 대두되고 있다. 미국의 국토안보부(DHS)는 효율적으로 사이버위협에 대응하기 위하여 2012년부터 규격 개발에 착수하여, MITRE를 통해 2013년 4월에 사이버 위협정보 전송 규격(TAXII), 10월에는 사이버 위협 표현 규격(STIX)을 발표함으로써 각 보안 시스템 간 연계를 표준화 하였는데, 국내 또한 최근에는 Restful API를 이용하여 보안 시스템 간 연계를 시도하고 있는데, 아직까지는 서로 표준화 되어 있지 않아 위협정보를 공유하고 대응하는데 어려움이 있다.

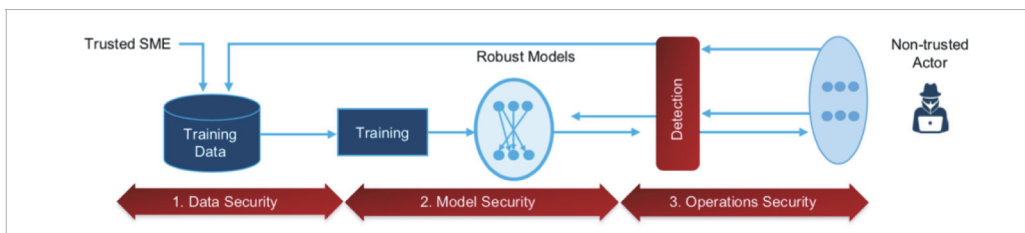
※ MITRE: 미연방정부의 지원 하에 R&D사업을 증진하는 비영리단체

※ STIX: 개별 조직들이 보유하고 발전시켜 온 사이버 위협 정보의 개념을 표준화하고 구조화하여 사이버 위협에 대한 일관된 분석과 자동화된 해석이 가능하게 한 정보 표현 규격

※ TAXII: STIX로 표현된 사이버 위협 정보를 실시간으로 공유하기 위한 자동 전송 규격

둘째, 인공지능 자체에 대한 보안위협 (적대적 인공지능: Adversarial AI) 이 현실화 되고 있으며, 이에 대한 대응방안 필요하다. 인공지능 기술이 발달하면서 기술의 활용범위가 지속적으로 확대되고 있지만, 일각에서는 이로 인해 발생 가능한 보안 위협 우려하고 있다. 인공지능에 대한 보안위협으로는 공격자가 AI를 활용하여 기존 공격 방식을 고도화하거나 새로운 방식의 공격 수행하는 인공지능을 활용한 공격, 공격자가 인공지능 시스템을 교란시키는 인공지능을 노린 공격으로 대표적으로 적대적 예시, 데이터 중독, 은닉음성 명령 등이 있다.

[그림] 인공지능에 대한 보안위협

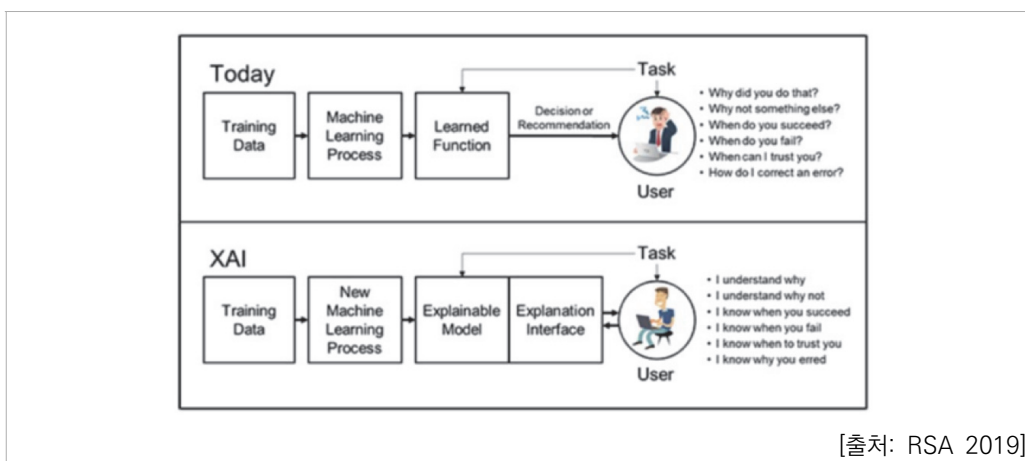


이에 인공지능을 활용하여 기존 공격방식을 고도화하거나 새로운 방식의 공격을 수행할 수 있으며, 동시에 인공지능시스템을 교란시키는 방법 등이 등장할 수 있음. 현재, 인공지능을 도입하여 활용하거나 도입계획이 있는 곳은 인공지능을 통해 발생 가능한 보안위협에 대한 지속적인 모니터링 및 보완이 필요하며, 현 정보보호시스템에 대한 보안성 검토 및 인증 제도에 대한 검토 등이 필요하다.

셋째, 설명 가능한 인공지능 (eXplainable AI, XAI)에 대한 지속적인 연구 및 적용이 필요하다. 인공지능 기술(머신러닝 등)은 빅데이터 및 복잡한 알고리즘 등을 기반으로 사용자에게 의사결정, 추천, 예측 등의 정보를 제공하지만, 일부 머신러닝 기술(딥러닝 등)은 알고리즘의 복잡성으로 인해 ‘블랙박스’라 불리며, 도출한 최종 결과의 근거, 도출 과정의 타당성 등을 제공하지 못하는 이슈가 존재한다. 이에 사용자가 인공지능 시스템의 동작과 최종 결과를 이해하고 올바르게 해석하여 결과물이 생성되는 과정을 설명 가능하도록 해주는 기술이 필요하다.

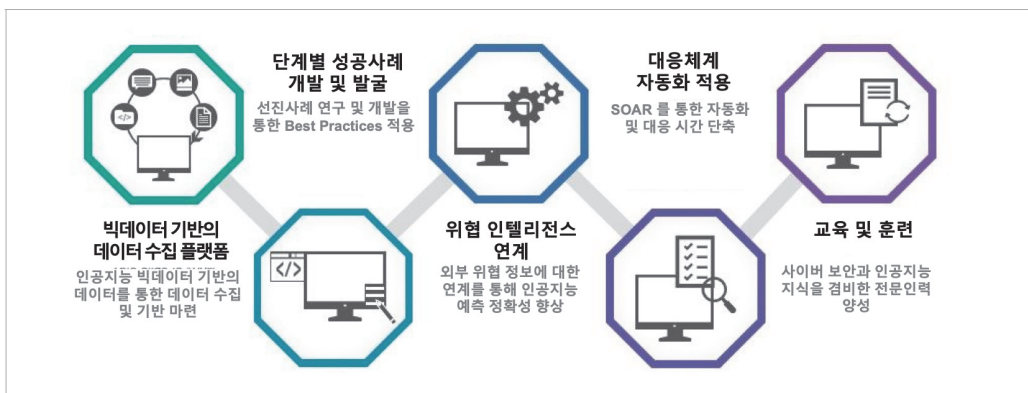
※ 미(美) 국방성 산하 국방위고등연구계획국(DARPA)에서는 ‘17년부터 XAI 관련 프로젝트 (XAI 학습 모델 개발 및 테스트)를 추진

[그림] 설명 가능한 인공지능에 대한 설명



설명 가능한 인공지능 (XAI)을 위한 기술적 접근방법으로는 기존 학습 모델 변형, 새로운 학습 모델 개발, 학습 모델 간 비교에 기반을 둔 방법이 있다. 현재, 이 기술에 대한 연구는 초기단계이지만, 보안기술 분야에 인공지능을 적용함으로써 인공지능을 통한 보안기술 향상, 위협에 대한 새로운 인사이트 습득, 해킹 공격에 대한 능동적인 대응 등의 효과가 기대할 수 있다. 만약, 인공지능을 통해 도출된 결과에 대한 명확한 설명 및 분석이 어려우면 분쟁 및 악용 될 소지가 있으므로, 지속적인 개선 및 개발이 필요한 부분이다.

[그림] 인공지능 보안기술 적용 시 고려사항



인공지능 보안기술 적용 시 고려사항

인공지능 보안기술 적용 시 효율성과 정확성을 극대화하기 위해서는 다음과 같은 부분을 고려하여야 한다.

첫째, 인공지능 기반의 보안기술을 적용하기 위해서는 관련 데이터에 대한 수집 영역에 대한 고려가 필요하다. 이를 위해 최근 다양한 분야에 적용된 빅데이터 기반의 보안 데이터 수집 플랫폼과 연계를 하거나 활용하는 방안이 필요하다. 기존의 보안장비에서 수집하고 있는 보안데이터, 침해사고 데이터, 악성코드 데이터 등 기존의 사이버 보안 업무에서 수집 활용한다. 예를 들면 기존 보안관제센터를 운영하고 있는 곳에서는 빅데이터 기반의 보안관제시스템 또는 통합로그관리 시스템 등을 통해 수집된 데이터 활용, 한국인터넷진흥원(KISA), 과기부 등을 통해 보안에 필요한 데이터셋을 구매 또는 수집하여 국가적으로 관리, 비용 부담 및 전문성 부족 등으로 데이터 활용에 어려움을 겪는 중소기업들을 지원하기 위하여 데이터 구매 및 가공 지원 사업 추진 등이 있다.

※ 국내 시장은 양질의 데이터 부족, 취약한 기술기반, 낮은 데이터 이용률 등 한계에 직면 : (개방 공공 데이터량) 한국 2.5만개, 미국 23.3만개 / (빅데이터 기술수준) 미국대비 79% 수준 / 국내 기업의 빅데이터 이용률 7.5%(17년)

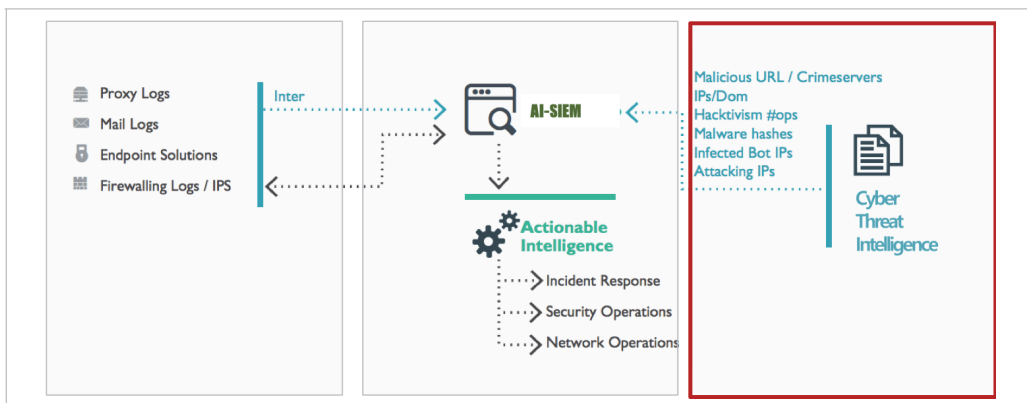
둘째, 편익을 가속화하고 극대화하기 위해 다양한 분야의 성공 사례를 개발하고 발굴하는 게 필요하다.

인공지능 기반의 보안기술이 제품과 사업에 안정적으로 적용되기 위해서는 시간과 다양한 활용사례들이 필요하다. 이는 성공한 사례 뿐 아니라 미흡한 사례까지 철저히 분석하여 지속적으로 최적의 결과에 도달하기 위한 반복 수행이 필요하다. 실제로는 사이버 보안에 인공지능을 적용하기 위해서는 현재, 수행되고 있는 모든 분야가 아닌 인공지능을 활용할 수 있는 분야와 범위를 선정하여 점진적으로 확대해 나가는 게 필요하다.

셋째, 대외적인 협업 및 위협정보 공유를 통해 인공지능 시스템의 정합성 향상이 필요하다.

SIEM 등 빅데이터 기반의 보안시스템에서 수집 예측된 데이터에 대해 위협 정보를 연계함으로써 인해 예측 값에 대한 정합성 향상 시킬 수 있으며, 이는 보안장비에서 발생한 보안이벤트에 대한 AI 예측 값과 외부에서 발생한 위협정보를 연계함으로써 예측 값에 대한 정합성 향상할 수 있음을 말한다.

[그림] SIEM과 CTI 연계 화면



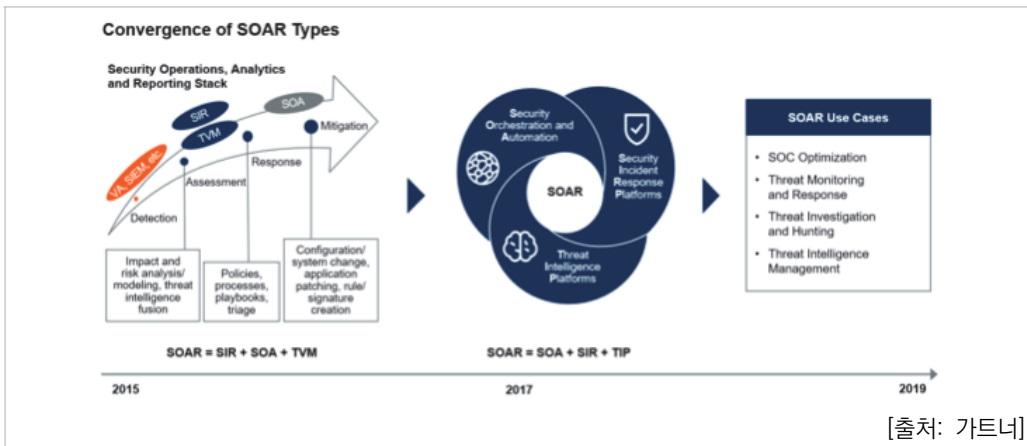
넷째, 보안 관리를 향상하기 위해 SOAR(Security Orchestration, Automation, Response) 적용하여 대응체계 자동화 및 대응시간 단축 효과를 얻을 수 있다. SOAR를 통해 인공지능이 적용된 보안기술을 더욱더 효율적으로 사용할 수 있게 할 수 있으며, 이로 인해 인공지능이 보안 기술에 녹아들기 위해서는 SOAR 구현이 필수적이다.

※ SOAR는 다양한 보안 위협에 대한 대응 프로세스를 자동화해 낮은 수준의 보안 이벤트는 사람의 도움 없이 처리하고, 보안사고 발생 시 표준화된 업무 프로세스에 따라 직원이 쉽게 대응할 수 있게 도와주는 보안솔루션임. 가트너에 따르면, SOAR은 세 가지 기능을 제공한다. 가장 중요한 기능은 '자동화'이다. SOAR은 자동으로 위협 의심 정보를 식별하고 판단해 업무를 줄여준다. 그뿐만 아니라, 기관 내 구축된 보안 솔루션에 자동으로 보안 정책을 내려주는 기능도 제공

또한, 이를 위해서는 각 보안 솔루션간의 연계를 위해서는 STIX/TAXII 와 같은 사이버위협 정보공유체계가 기본이다.

※ STIX/TAXII Support List : <https://stixproject.github.io/supporters/>

[그림] SOAR 유형



마지막으로 보안 분야에서 인공지능을 효율적으로 활용하기 위해서는 보안전문가를 위한 맞춤형 인공지능 교육 필요하다. 인공지능의 효율적 사용을 위해서는 가장 중요한 것은 인공지능에 대한 지식과 도메인 지식이다. 이미 보안전문가는 관련 보안에 대한 지식을 충분히 가지고 있는 상황에서 이들에 대한 맞춤형 보안에 필요한 인공지능 관련 교육을 사이버 보안에 맞게 하는 게 필요하다.

지금까지 인공지능 보안기술에 대한 현황 및 대두될 이슈, 다양한 고려사항에 대해 알아보았다. 필자가 느끼기에는 인공지능(기계학습)을 보안기술에 적용하려는 시도는 지속적으로 계속되어왔으며, 이중 성공하여 안정적으로 정착된 분야도 있고, 그렇지 않은 분야도 있다. 이러한 관점에서 보면 지금까지는 기술이 사람에게 맞추는 시대라면, 이제는 사람이 기술에 맞추어야 되는 시기가 되지 않았을까 한다. 특히, 지금 이 시기(인공지능, IoT 등)는 말이다.

이글을 쓰면서 필자는 1903년에 라이먼 프랭크가 쓴 오즈의 마법사라는 책이 생각이 되었다.

지금 우리에게도 허수아비가 구하려고 했던 지혜, 양철 나무꾼이 가지고자 했던 심장, 겁쟁이 사자가 갖고 싶어 하던 용기가 보안솔루션 개발자, 보안정책담당자, 정보보안담당자 등에게 꼭 필요하지 않을까?

결국 오즈의 마법사에 등장하는 주인공들이 모든 역경을 극복하고 자신이 원하는 것을 얻었듯이 우리도 사이버위협으로부터 우리의 자산을 안전하게 보호할 수 있을 것이다.

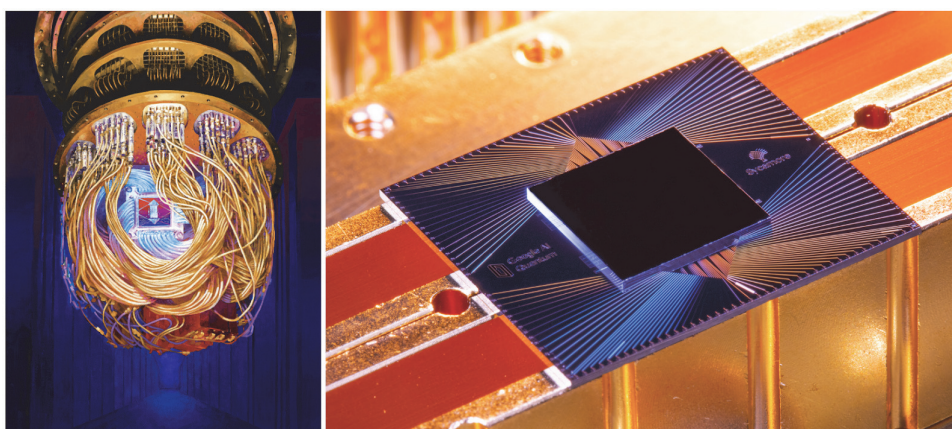
양자암호통신과 보안의 미래

국가보안기술연구소, 권대성 센터장
국가보안기술연구소, 장진각 팀장

1. 양자정보통신

양자정보통신 분야에서 최근 가장 주목받는 뉴스는 2019년 10월 Nature 지에 게재된 구글의 “Quantum supremacy using a programmable superconducting processor”이란 논문 발표이다. 이 논문에서는 초전도체 프로세서를 가진 양자컴퓨터가 슈퍼컴퓨터의 계산능력을 추월하기 시작한 것을 설명한다. 이제 양자컴퓨터의 시대가 바로 눈앞에 다가와 있음을 보여주고 있다.

[그림] Google AI Blog: Quantum Supremacy Using a Programmable Superconducting Processor



[출처: <https://ai.googleblog.com/2019/10/quantum-supremacy-using-programmable.html>]

양자컴퓨터라는 신기술의 발전은 많은 논문 및 뉴스들로부터 확인할 수 있다. 미국, 중국, 유럽 등 국가 중심의 대규모 프로젝트 및 투자가 진행 중이며, 구글, IBM, 마이크로소프트사 등 대형 글로벌 ICT 회사들이 투자를 하고 있다. 대학에 속해있던 많은 양자기술 전문 연구자들이 산업체로 이동하는 현상은 양자컴퓨터 기술의 실용화가 다가오고 있음을 잘 보여준다.

양자기술 연구 초기부터 지금까지 가장 많이 언급되는 내용은 양자컴퓨터가 개발되면 현대 암호체계가 쉽게 해독된다는 것이다. 엄밀하게 말하면, 전자상거래, 공인/사설 인증체계의 핵심인 RSA, 타원곡선암호 등 공개키 암호를 양자컴퓨터가 쉽게 해독할 수 있다는 사실이다. 현대 암호체계의 중요한 두 개의 축인 비밀키암호와 공개키암호 중 공개키암호에 해당하는 내용으로, 현대 암호체계 자체가 무너지는 일과는 무관하다. 그러나 공개키암호의 해독만으로도 현 인터넷 체계의 안전성을 무너뜨리는 대단한 사건이 될 수 있다. 또한 공개키암호 기술은 인터넷체계에 보급되는 과정에서부터 인프라 성격을 가지고 있다. 즉 한번 보급된 공개키암호 체계는 쉽게 바꿀 수 없어 사전 대처가 필요한 부분이기도 하다.

양자를 이용한 ICT 연구의 핵심인 양자컴퓨터의 위협에 대해 양자를 이용하여 막고자 하는 기술도 있다. 공개키암호의 주요 기능 중 하나인 키분배 기능은 80년대 중반에 개발된 양자키분배라는 기술로 제공할 수 있다. 양자키분배 기술은 빛의 양자인 광자로 정보를 전달하되, 실시간으로 도청을 검출할 수 있는 특징을 가지고 있다.

양자키분배는 양자컴퓨터 이론이 개발되는 2000년대 초반부터, 양자분야에서 당장 실현할 수 있는 기술로 연구 및 홍보가 많이 이루어졌다. 양자키분배 외에도 양자를 이용하여 다른 암호기능들을 제공하는 연구도 지속적으로 이루어지고 있다. 또한 양자를 이용한 통신체계를 포함하여 양자암호통신이라고 말한다.(연구개발 초기인 현재 양자키분배 만으로 양자암호통신이라 부르는 경향이 있다.) 양자암호통신과 양자컴퓨터 외에도 양자센서 및 메트롤로지 기술을 포함하여 양자정보통신이라고 부른다.

본 고에서는 양자정보통신 기술 중 양자키분배가 주를 이루고 있는 양자암호통신의 의미를 살펴보고, 양자암호통신과 보안의 미래에 대하여 조망해본다.

2. 양자암호통신의 의미

암호기술은 고대로부터 연구되어 왔으며, 2차 세계 대전 중 독일군의 에니그마 암호의 해독은 컴퓨터의 발전과 이를 이용한 암호의 발전을 가져왔다. 다시 말하면, 컴퓨터의 개발로 인하여 2차 세계대전 전까지 쓰이던 암호들의 해독이 쉬워지고, 지금의 현대암호가 개발되는 계기가 되었다.

1976년 두 수학자 W. Diffie와 M. Hellman이 “New Directions in Cryptography”라는 논문을 통하여 인터넷을 이용한 암호키분배 기술을 발표하였다[5]. 기존의 암호들은 단순한 수학을 이용하여 암호를 풀지 못하도록 고안한 반면, 이 논문은 정수론을 암호에 도입하여 공개적으로 키를 전달할 수 있는 방법을 제시하였다. 이 방법이 바로 공개키 암호방식으로, 암호기술에 매우 중요한 변화를 가져왔다. 이 논문이 없었다면

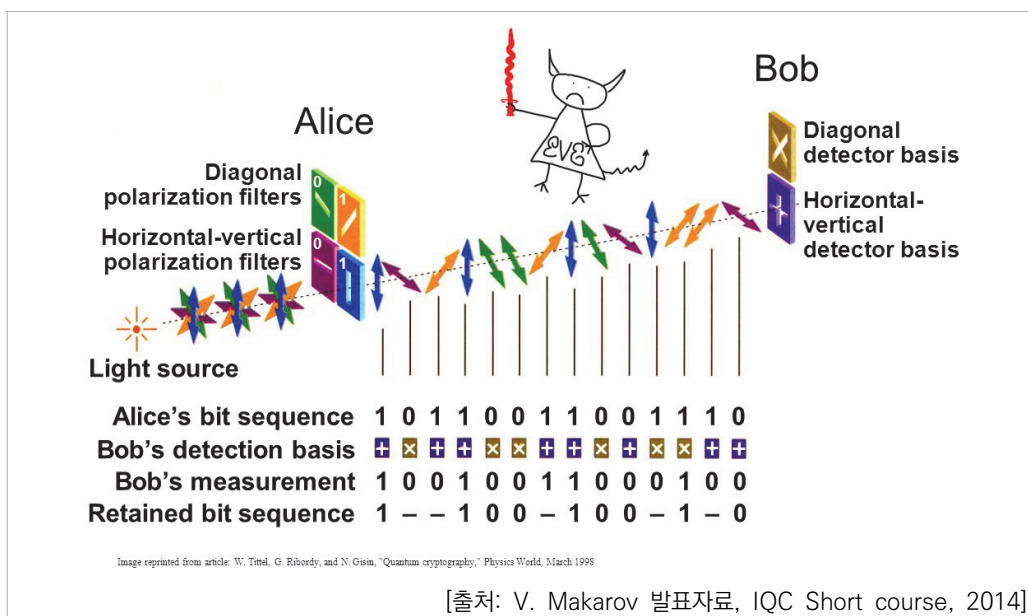
아마도 인터넷이 지금처럼 활성화되지 못하고, 많은 취약점을 보이면서 보급에 어려움을 겪었을 수도 있었을 것이다.

이를 계기로 정수론의 문제들을 이용하여, 데이터 암호화 및 전자서명을 가능하게 하는 RSA암호, 타원곡선 암호가 1978년, 1985년 개발되었다. 특히 이 새로운 암호기술을 활용한 전자서명 기능은 인터넷에서 상대방을 확인할 수 있는 기반을 제공하는 획기적인 기술이기도 하다. 공개키 암호기술은 현재의 전자상거래 보안의 근간을 형성하고 있다.

컴퓨터 등장이 현대암호를 만들었다면, 양자 컴퓨터의 등장은 또 다른 암호 패러다임을 가져올 것이다. 가장 큰 변화는 양자 컴퓨터의 등장으로 쉽게 해독될 수 있는 공개키암호, 전자서명 분야이다.

양자를 이용한 암호기법 연구에서 가장 많이 언급되고, 이러한 연구의 실질적 시초라고 볼 수 있는 것은 1984년 물리학자 C. Bennet과 암호학자 G. Brassard가 발표한 “Quantum cryptography(Public key distribution and coin tossing)”에서 시작된 BB84 프로토콜이다.

[그림] BB84 프로토콜



이 BB84 프로토콜은 수학 대신 양자역학을 이용하고 있는데, 두 사람이 양자(여기서는 광자)를 이용하여 암호키를 안전하게 분배 및 교환할 수 있다. 이 방식은 기존 암호와 달리 양자역학에 기반하고 있어, 양자컴퓨터를 이용한 해독, 중간에 가로채기 및

끼어들기 공격이 전혀 적용되지 않아 높은 안전성을 제공할 수 있다는 장점을 가지고 있다.

이와 같이 양자를 이용한 암호키 분배기법들을 양자키분배(Quantum Key Distribution)라고 한다. 수학적 계산으로 이루어지는 기존 암호들과는 달리, 양자키분배는 양자를 생성하고 탐지하는 과정으로 구성된다. 이를 위해, 양자를 제어할 수 있는 전용 하드웨어가 필요하고, 이 전용 하드웨어가 연결되는 양자채널을 사용한다. 아직까지 양자를 다루는 소자기술에 한계가 있어, 양자키분배의 이론과 구현이 정확히 일치하지는 않는 특징도 있다.

2000년 초반부터 양자컴퓨터 위협이 대두되었지만, 그 이후 상당기간 양자컴퓨터 발전이 크게 이루어지지 않아, 양자키분배 기술의 실용화는 큰 진전이 이루어지지 않았다. 그러나 최근 양자컴퓨터의 발전이 급진전함에 따라, 각 국에서는 양자키분배 기술을 실망에 적용하는 것을 고려하기 시작하였으며, 기술의 실제성을 확인하기 위한 시험망들을 운영하고 있다. 상용 수준의 양자키분배 장치 개발 사례도 증가하고 있다. 양자키분배 장치는 현재 IDQ(스위스), Toshiba(일본), MagiQ(미국), Quantum CTek, QAsky(중국), SKT 등 다양한 회사에서 상용화 혹은 상용화 준비를 진행하고 있다.

양자키분배 기술과 관련된 최근의 뉴스에서는 양자암호통신이 대표용어로 나오고 있다. 엄밀하게 말하면, 양자암호통신은 양자를 이용한 암호통신이라고 정의하며, 암호 기술과 통신기술을 모두 다루고 있다. 그렇지만, 양자를 기반으로 하는 암호기술은 키 분배에 국한되고 있으며, 실제 암호화(비밀키암호), 인증(공개키암호)은 양자컴퓨터에도 안전한 현대 암호로 이루어지는 혼합방식이 채택되고 있다. 요즘 많은 언론기사에서 접할 수 있는 양자암호통신은 양자키분배와 현대암호를 이용한 암호통신을 함께 다루는 것이다.

이런 의미에서 볼 때, 현재의 양자암호통신은 지금의 암호통신을 완전히 변화시키는 개념은 아니며, 양자컴퓨터에 해독될 수 있는 공개키암호가 담당하는 키분배 기능을 양자키분배로 대체하는 것이다.

즉, 현재의 양자암호통신은 양자를 이용한 키분배 기능과 현대암호 중 양자컴퓨터를 이용한 공격에 안전한 암호화 기능을 결합하여, 양자컴퓨터 및 슈퍼컴퓨터 발전에 무관한 안전성을 갖춘 암호체계를 제공한다. 이 양자암호통신을 사용하면 현재 사용되는 기존 암호들보다 한단계 높은 안전성을 제공할 수 있게 된다.

양자키분배 기술의 현 실태를 제대로 보기 위해서는 미국 NIST에서 공모사업을 진행하고 있는 양자내성(공개키)암호 프로젝트(Quantum-safe/post-quantum cryptography)와 비교가 필요하다. 양자내성암호는 현 암호체계 틀에서 양자컴퓨터를 이용한 공격에

도 안전한 새로운 공개키암호를 의미한다.

양자키분배 및 양자내성암호라는 두 기술 모두 양자컴퓨터를 이용한 암호해독 위협을 해소하기 위해 현재 개발되고 있다. 양자키분배는 컴퓨팅의 발전에 관계없는 안전성을 제공하고, 키분배 내용을 가로채서 저장하고 오프라인으로 암호키를 얻는 통산적인 암호 공격을 적용할 수 없다는 장점을 가지고 있다. 반면 양자내성암호는 양자키분배처럼 전용 하드웨어가 필요하지 않고 소프트웨어로 다양한 디바이스에서 구현될 수 있고, 키분배를 위한 별도의 채널이 필요하지 않은 장점이 있다.

양자키분배 기술은 적용 환경(별도 광학채널), 비용, 현재 암호통신과의 결합 용이성, 다양한 공격기법에 대한 안전성 확보, 이들을 고려한 표준화 등이 부족하다. 양자내성 공개키암호는 여러 가지 방식으로 진행되고 있는데, 아직 양자컴퓨터를 위한 안전성 분석이 이루어지지 않았고, 여전히 수학적 복잡도에 의존하고 있어, 컴퓨팅 파워, 해독 알고리즘 발전에 의하여, 안전성이 지속적으로 저하될 수 있다.

양자키분배 기술은 양자컴퓨터 위협에 대응하여, 기존 공개키 암호 시장을 대체할 수 있다는 장점이 있으나, 전자서명 등의 암호 핵심기능을 현재는 지원할 수 없고, 다양한 환경에 적용되는 데는 한계가 있어, 아직까지 공개키암호와의 공존이 필요하다.

3. 양자암호통신의 현재

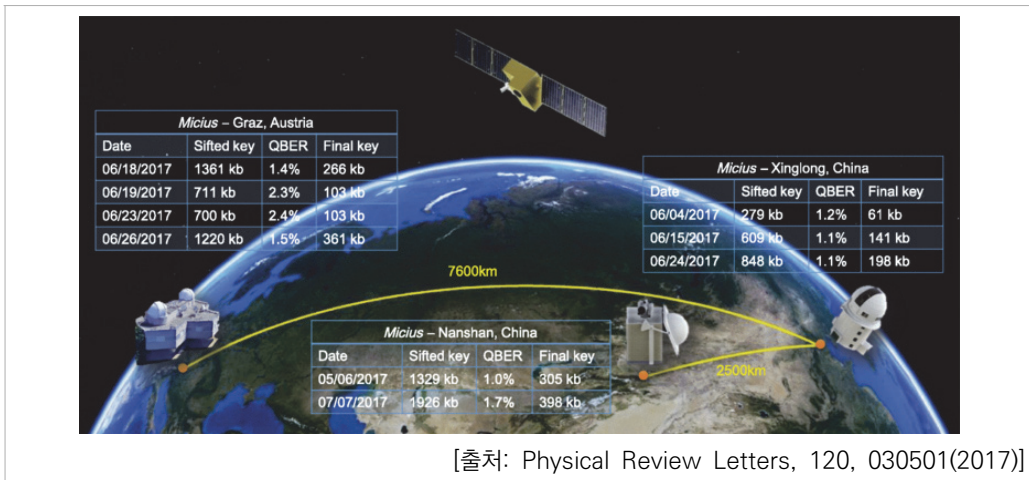
양자암호통신, 정확히는 양자키분배를 통신망에 적용하기 위해서는 이를 위한 장치 개발 및 표준화가 필요하다.

양자키분배 장치는 현재 IDQ(스위스), Toshiba(일본), MagiQ(미국), Quantum CTek(중국), SKT 등 다양한 회사에서 상용화 혹은 상용화 준비를 진행하고 있다. 상용화 기술은 단일광자 생성의 어려움을 극복하기 위해 고안된 디코이 적용 BB84 프로토콜 구현시스템이 대부분이며, 대체적으로 50km 내외의 전송거리에서 최적 키생성률이 제시되고 있다.

양자키분배 기술은 기존 광통신과는 달리 하나의 광자를 직접 제어하기 때문에, 기존 통신망에서의 활용 가능성을 확인하는 시험망이 다양하게 만들어져 왔다.

한편, 중국은 '중국이 세계를 선도하는 과학기술' 중의 하나로 양자기술을 선정하여 집중적인 연구개발 투자를 지속하고 있으며, 최근에는 괄목할만한 결과들을 만들어내고 있다. 그 중 유선 양자키분배 분야에서는 2017년에 2,000km에 달하는 양자암호 기간통신망을 개통하여 운영 중이며, 2016년 세계 최초로 양자 위성인 목자호를 성공적으로 발사하였고, 2017년 이 위성을 이용한 무선 양자키분배 역시 성공하였다.

[그림] 중국의 위성 양자키분배 결과



국내에서는 2009년 이 후, SKT 주도로 양자키분배 기술 개발이 활발하게 진행되고 있다. 특히 SKT는 2018년 세계적인 양자키분배 벤처회사인 ID Quantique(이하 IDQ)를 인수하여 양자기술 사업화 및 상용망 시장 선점에 나서고 있다. 양자키분배 장치 개발은 IDQ 중심, 표준화는 SKT 중심으로 이원화하여 추진하고 있다. 또한, KT는 양자키분배 개발체계 기반확보에 나서고 있으며, ITU-T 국제표준화에 집중하고 있다.

성공적인 기술개발 보고와는 별개로, 양자키분배 기술이 해결해야할 과제도 여전히 남아있다. 주요 구현 문제는 ① 안정적 단일광자 생성, ② 수신 디바이스의 감지 오류, ③ 광원의 도달거리(상용 광통신망 약 100km 내외) 등으로 좁혀질 수 있다. 이러한 문제를 해결하기 위한 단일광원, 고성능 저가형 단일광자 측정기, 양자리피터 등의 기술 개발이 지금도 진행 중이다.

[표] 주요 회사의 양자키 분배 시스템

회사명	Toshiba	IDQ	NEC	QAsky	Quantum CTek	SKT
Key Rate	13.72Mbps @10km	1.42kbps @50km	112.4kbps @22km	40kbps @50km	50kbps @50km	10kbps @50km
Key Rate@50km	2.17Mbps	1.42kbps	40kbps	40kbps	50kbps	10kbps
Protocol	Decoyed BB84	COW	Decoyed BB84	Decoyed BB84	Decoyed BB84	Decoyed BB84
Encoding	Phase	Time-bin	Phase	Phase	Polarization	Phase

[출처: Toshiba (2017 ETSI Quantum Workshop 발표)]

양자키분배 장치의 실망 운용을 위해서는 상기 구현 한계에 따른 문제들과 더불어 암호시스템 공격기술인 각종 물리적/SW적, 지능적 공격 등에 대해서도 충분한 검토가 요구된다. 이와 같은 다양한 안전성 문제는 양자키분배 장치의 안전한 사용체계 확보를 위해 기술적으로 해결되어야 하며, 그 결과는 국제적으로 승인된 표준화로 연결되어야 한다. 실제로 현재 사용되는 암호통신기술은 모두 국제 표준에 명시된 절차를 따라 구현 및 검증되고 있으며, 양자키분배 역시 기술의 상용화를 위해 이와 같은 절차를 확보해야 한다.

양자키분배 표준화에 대한 검토를 앞서서 진행한 곳은 유럽 표준협회인 ETSI (European Telecommunications Standards Institute, 유럽전기통신표준협회)이다. ETSI는 양자키분배 위원회를 두고 있으며, 7개의 GS(Group Specification)와 2개의 GR(Group Report)을 출판하고 갱신하고 있다.

[표] 양자키분배 관련 ETSI 출판물

출판명	제목
ETSI GS QKD 012 V1.1.1	Quantum Key Distribution(QKD): Device and Communication Channel Parameters for QKD Deployment
ETSI GS QKD 014 V1.1.1	Quantum Key Distribution(QKD): Protocol and data format of REST-based key delivery API
ETSI GR QKD 007 v1.1.1	Quantum Key Distribution(QKD): Vocabulary
ETSI GR QKD 003 v2.1.1	Quantum Key Distribution(QKD): Components and Internal Interfaces
ETSI GS QKD 011 V1.1.1	Quantum Key Distribution(QKD): Components characterization: characterizing optical components for QKD systems
ETSI GS QKD 005 V1.1.1	Quantum Key Distribution(QKD): Security Proofs
ETSI GS QKD 008 V1.1.1	Quantum Key Distribution(QKD): QKD Module Security Specification
ETSI GS QKD 004 V1.1.1	Quantum Key Distribution(QKD): Application Interface
ETSI GS QKD 002 V1.1.1	Quantum Key Distribution(QKD): Use Cases

[출처: 유럽표준협회(ETSI) 홈페이지]

국내에서는 TTA(Telecommunications Technology Association, 한국정보통신기술협회)에서 표준화를 진행하고 있는데, 통신망 기술위원회(TC2)에서는 ETSI 문서 도입표준을, 정보보호 기술위원회(TC5)에서는 국가공공 도입에 필요한 프로토콜 규격과 보안 요구사항을 독자적으로 개발하고 있다.

[표] 양자키 분배 관련 TTA 표준화

표준번호	표준명
TTAK.KO-12.0329-Part1	양자키분배: 제 1부: 일반
TTAK.KO-12.0329-Part2	양자키분배: 제 2부: BB84 프로토콜
TTAK.KO-12.0356	양자키분배: 보안요구사항
TTAE.ET-GS QKD 008	양자키분배: 모듈보안규격
TTAE.ET-GS QKD 011	양자키분배: 구성요소특성화: QKD시스템의 광학구성요소 특성화
TTAE.ET-GS QKD 004	양자키 분배망: 응용 인터페이스
TTAE.ET-GS QKD 003	양자키분배: 구성요소 및 내부인터페이스

[출처: TTA]

ISO/IEC에서는 중국이 표준화 추진에 앞장서고 있다. 암호키분배 관련 표준은 TTA 표준에서처럼 크게 두 가지로 분류된다. 프로토콜 동작 규격을 정하는 암호 알고리즘과 이를 암호모듈에서 안전하게 운용하기 위한 보안 요구사항(또는 평가기준)으로 나뉜다. 일반적인 표준화 절차는 암호 프로토콜(알고리즘) 표준화가 선행된다. 그러나 ISO/IEC의 암호 알고리즘 표준화 그룹에서는 이를 지지하고 있지 않아서, 중국 등은 규격이 명시되지 않은 평가 기준 표준화만을 추진하고 있다. 2017년 가을 독일 회의에서 표준화 추진이 제안되었고, 2019년 봄 이스라엘 회의에서 정식 표준화 과제로 채택되었다.

[표] 양자키 분배 관련 ISO/IEC JTC 1/SC 27 표준화

프로젝트 번호	제목
23837-1	Security requirements, test and evaluation method for qkd-Part 1. Requirements
23837-2	Security requirements, test and evaluation method for qkd-Part 2. Test and evaluation methods

한편, ITU-T에서는 양자키 분배 활용 및 양자난수발생기 구조에 대한 다양한 표준화를 SG13과 SG17에서 진행하고 있다. ITU-T의 국제표준화는 KT(SG13) 및 SKT(SG17)가 문서개발 주관을 맡아 표준화 활동을 주도하고 있다.

ISO/IEC 표준화는 프로토콜을 특정하지 않는 평가방법을 대상으로 하고 있어 보안성 검토에 한계가 있을 것으로 보이며, ITU-T 표준화는 다양한 의견 제기 단계이다.

암호키분배는 암호시스템에 있어서 핵심적인 안전성을 제공하는 요소이므로, 충분한 검토 및 객관적 신뢰성 확보가 필요한 부분이다. 암호에서 키분배의 취약점은 정보

시스템 전체의 붕괴로 연결될 수도 있기 때문에, 암호를 주도하고 있는 미국 등에서는 양자키분배의 표준화에 신중을 기하고 있다.

4. 양자암호통신의 미래

현재 양자키분배 기술은 실용화를 위한 단계를 서서히 거치고 있으며, 기존 현대암호 기법들은 발전하고 있는 컴퓨팅 파워 및 해독 기법들로 인하여 장기간 안전성 확보를 자신할 수 없는 만큼, 특정 영역을 중심으로 적용이 확대될 것으로 예상된다.

유선으로는 양자리피터 등의 개발과 함께 연결 거리를 확대할 수 있을 것이며, 중국 등이 성공한 인공위성을 이용한 무선 양자키분배 기술과도 결합될 것이다.

앞에서 언급했듯이, 현재의 양자암호통신은 양자키분배와 현대암호의 암호화 기능이 결합된 형태이다.

장기적으로 보면, 키분배 외에도 양자를 이용한 인증, 서명, 암호화 기법들도 양자컴퓨터 발전과 더불어 개발될 것으로 보인다.

향후, 네트워크가 양자네트워크로 발전하고, 컴퓨터가 양자컴퓨터로 발전한다고 예상되는 만큼, 이 틀에서 암호통신은 결국 양자기반의 암호통신으로 발전해야 할 것으로 예상된다.

산업적인 측면에서 보면, 양자암호통신은 양자컴퓨터를 이용한 해독위협에 안전성을 제공하기 위한 암호통신 기술의 하나로 사용될 것이다. 세부적으로는 암호키를 분배하는 양자키분배 기술과 실제 데이터의 고속 암호화를 담당하는 비밀키 암호, 현재 전자서명을 대체하고 양자컴퓨터 해독위협에 내성을 가지는 전자서명 등이 암호학적으로 안전하게 결합되고, 구현 안전성이 충분히 검증되어진 후 새로운 시대의 암호통신 기술로 자리할 것이다.

5. 맺음말

양자암호통신은 양자컴퓨터 및 양자통신으로 대표되는 미래 ICT환경으로 가기위한 암호통신기술이자, 현대암호체계와 결합하여, 현 ICT에서 활용할 수 있는 암호통신기술이다.

특히, 도청에 대한 안전성, 중간자 가로채기/끼어들기 공격 등에 대해서는 기존 암호보다 매우 뛰어난 안전성을 가진다. 그러나, 산업적 측면에서는 이러한 특성이 기존의 암호통신을 양자암호통신으로 전면적인 대체를 하게 만드는 사유가 되지는 않는다. 컴퓨터의 개발 이후 암호가 상업적으로 활용되기까지 많은 시간이 소요되었다. 인터넷

체계에 암호통신기술이 일부가 되는 과정, 암호통신 인프라가 구축되는 과정 등 많은 기술적 성숙의 결과가 현재의 암호통신체계이기 때문이다.

양자컴퓨터의 개발 및 양자 네트워크기술 발전은 암호통신체계의 변화를 촉발할 것으로 예상되지만, 현재의 양자암호통신이 이러한 변화를 주도할 수 있는 것은 아니다. 양자암호통신이 필요한 분야에서부터 점진적으로 설치, 확장되고, 구현 안전성이 확보되었다고 모두가 인정할 수 있어야 한다. 이와 같이 양자암호통신 기술력에 대한 공감대를 확대하고, 발전하는 양자 ICT와 보조를 같이 하여야, 변화하는 암호통신체계에 대한 요구 속에서 양자암호통신이 자리 잡는 데 많은 도움이 될 것이다.

참고문헌

- F. Arute 외, Quantum supremacy using a programmable superconducting processor, *Nature*, 574, 505(2019)
- National quantum initiative act, Public Law No. 115-368(Dec. 21, 2018), <https://www.congress.gov/bill/115th-congress/house-bill/6227>
- China to boost scientific and technological innovation, http://english.www.gov.cn/policies/latest_releases/2016/08/08/content_281475412096102.htm
- Quantum technologies flagship, <https://ec.europa.eu/digital-single-market/en/quantum-technologies>
- W. Diffie, M. Hellman, New directions in cryptography, *IEEE Trans. on Inform. Theory*, 22, 644(1976)
- NIST, Post-quantum cryptography, <https://csrc.nist.gov/Projects/Post-Quantum-Cryptography>
- C. Elliott, The DARPA quantum network, preprint, quant-ph/0412029(2004)
- A. Poppe 외, Outline of the SECOQC quantum-key-distribution network in Vienna, *Intern. Journ. Quant. Inf.* (2008)
- F. Xu 외, Field experiment on a robust hierarchical metropolitan quantum cryptography network, preprint, arxiv:0906.3576(2009)
- R. Hughes 외, Network-centric quantum communications with application to critical infrastructure protection, preprint, arxiv:1305.0305(2013)
- China opens 2,000-km quantum communication line,

<http://www.ebeijing.gov.cn/BeijingInformation/BeijingNewsUpdate/t1494836.htm>, 2017-10-1

- S. Liao 외, Satellite-to-ground quantum key distribution, Nature 549, 43(2017)

5G 시대의 위협과 보안

SK인포섹, 권혁재 수석

5G 시대의 시작

지난 4월 세계 최초로 국내에서 5G 네트워크 서비스가 시작됐다. 새로운 서비스 시작과 함께 구매한 5G 스마트폰은 아직 4G LTE로 연결되는 시간이 더 길지만, 5G로 전환되었을 때의 네트워크 접속 반응 속도와 데이터 다운로드 속도는 기대했던 것 이상을 보여준다. 지난 12월 24일 크리스마스이브에 5G 스마트폰으로 LTE와 5G 연결 시 속도를 테스트한 결과는 다음과 같다.

[그림] 현재 사용 중인 스마트폰으로 LTE와 5G 네트워크 연결 시 속도 테스트



5G의 이론 속도인 20Gbps와는 큰 차이가 있지만, LTE와는 비교할 수 없을 정도로 20배 이상 빠른 속도를 보여준다. 시간이 지날수록 5G 네트워크는 더 안정화되고, 지금보다 더 나은 서비스를 이용할 수 있게 될 것이다.

5G와 이전 세대 네트워크의 차이점을 비교할 때, 초고속, 초저지연, 초연결의 3가지 특징을 주로 얘기한다.

초고속

5G 네트워크는 이론상 최대 20Gbps의 속도로 기존 4G 네트워크보다 20배 빠르다. 우리는 이와 같은 속도의 개선을 통해 웨이브, 넷플릭스와 같은 OTT(Over The Top) 서비스에서 제공하는 초고화질 영상 스트리밍을 모바일 기기에서도 끊김 없이 감상할 수 있다. 더 나아가 구글, 엔비디아와 같은 기업들에서 준비 중인 게임 스트리밍 서비스가 활성화되면 더 이상 게임을 다운로드 하지 않고 음악이나 영화와 같이 스트리밍으로 즐기는 날이 올 것이다.

초저지연

5G의 지연시간은 1ms로 기존의 10분의 1 수준으로 떨어졌다. 지연시간은 특정 지점에서의 요청이 목표 지점에 도달하는 시간을 의미한다. 즉, 지연시간이 낮다는 것은 내가 전송한 데이터가 상대방에게 그만큼 빨리 도착한다는 것이다. 요청의 처리속도가 동일하다면 지연시간이 최소화되는 것이 전체 응답시간을 줄이는데 중요하다.

5G의 가장 큰 특징은 바로 초저지연에 있다. 지연시간이 왜 중요할까? 자율주행 기술로 보면 차량에 장착된 카메라, 레이더 등의 여러 센서 정보들과 주변 차량 및 도로의 교통 정보를 클라우드에서 종합적으로 해석하여 원격의 차량에 실시간으로 제동, 가속, 조향 등에 대한 명령을 내려야 한다. 이 때, 네트워크에 지연이 발생하면 큰 사고로 이어질 수 있다. 4G 네트워크를 이용할 경우 자율주행 차량이 위험을 포착해 급정거하면 제동거리가 1.4m인데 반해 5G 환경에서는 2.8cm 밖에 되지 않아 위험에 더 안전하게 대응할 수 있다.

유선 네트워크만큼의 낮은 5G의 초저지연 기술은 자율주행, 원격의료, 증강현실(AR, Augmented Reality) 등 빠른 응답이 필요한 기술 분야 발전에 기여할 것으로 기대된다.

초연결성

5G 네트워크의 최대 연결기기는 기존보다 10배 많은 ㎢ 당 100만 개의 기기를 연결할 수 있다. 스마트폰, 태블릿 등 일부 기기만 연결되던 환경에서 5G 네트워크로 인해 자동차, 가전, 웨어러블 기기, 센서 등 우리 주변의 모든 기기들이 서로 연결되는 진정한 사물인터넷(IoT, Internet of Things) 시대가 다가오고 있다. 시장조사 전문기관인 가트너는 인터넷에 연결되는 기기가 2020년 260억 개로 증가할 것으로 추정했다.

18세기 중반 증기기관으로 시작된 1차 산업혁명을 지나 우리는 지금 4차 산업혁명

시대를 맞이하고 있다. 4차 산업혁명은 인공지능과 사물인터넷 등의 기술을 축으로 한 초연결 사회의 시작이 될 것이며, 5G는 이를 위한 핵심 인프라 기술이 될 것이다.

5G 시대의 보안 위협

지속되는 발전으로 더 나은 기술이 나타나고, 4차 산업혁명과 같은 패러다임이 바뀌는 시기에는 새로운 위협들이 나타난다. 우리는 5G라는 한층 더 나은 시대에 돌입했지만 새로운 위협들과 함께 이전에도 존재했던 취약점들이 더 큰 위협으로 다가 올 수 있다. 5G의 초고속, 초저지연, 초연결이라는 기술 향상과 이를 통해 제공되는 많은 편리한 서비스들은 공격자들에게도 더욱 나은 환경을 제공하여 이전보다 큰 규모의 위협을 마주하고 있다.

공격자의 관점에서 보면, 5G 환경은 공격 및 탈취 대상인 취약한 사물인터넷 기기의 폭발적인 증가를 가져오고, 기업의 영업비밀, 개인의 프라이버시 정보와 같은 중요 데이터를 이전보다 더 빠르게 더 많이 탈취할 수 있는 환경을 제공할 수 있다.

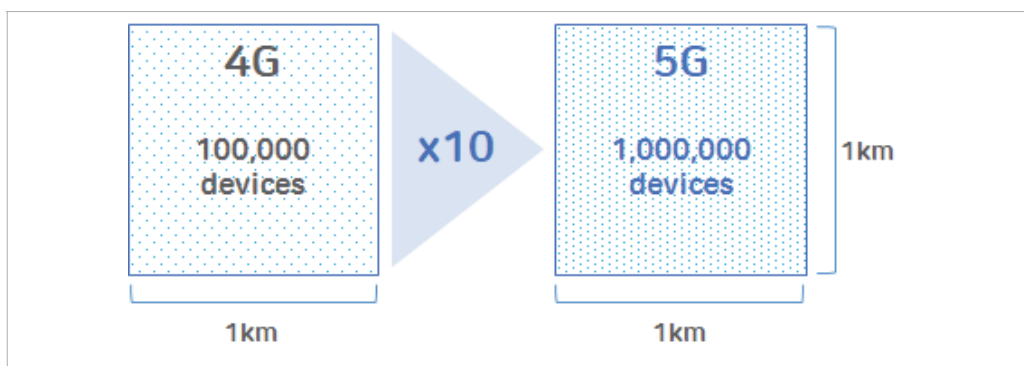
Massive IoT: 급격하게 늘어나는 스마트 기기들과 네트워크 연결

10년 전만 해도 인터넷에 연결해 사용하는 기기들은 노트북, 스마트폰, 태블릿 등 일부 기기들이었지만 지금은 스마트라는 이름을 붙인 수많은 기기들이 기하급수적으로 새롭게 출현하고 있다.

주변을 살펴보면 TV, 냉장고, 공기청정기, 조명, 스피커 등 가전부터 시계, 벨트, 신발 등 웨어러블 기기 그리고 심지어 체중계까지 스마트라는 이름을 붙이고 인터넷에 연결되고 있다. 해외 클라우드 펀딩 사이트인 킥스타터나 인디고고를 살펴보면 지금 이 순간에도 창의적이고 기발한 아이디어를 장착한 스마트 기기들이 개발 중이고, 이러한 기기들이 새롭게 네트워크에 연결되고 있다.

이전 네트워크 환경이 스마트폰 중심의 속도 및 성능 향상에 중점을 두었다면, 5G는 우리 생활 속의 모든 기기, 그리고 더 나아가 산업용 센서와 기기들까지 네트워크에 연결시키는 초연결 사회를 목표로 하고 있으며, 이를 Massive IoT로 표현한다. 사물인터넷을 이루는 기기들은 이전 세대 네트워크 환경에도 존재하였지만 5G를 통해 더욱 확산되고, 더 이상 트렌디한 기술이 아닌 생활·산업 전반에서 걸친 기반기술로서 자리 잡으며 폭발적으로 증가하고 있다.

[그림] 4G와 5G의 기기 연결 수의 변화



5G는 1km² 당 이전 4G 대비 10배 많은 100만대의 기기를 연결할 수 있다

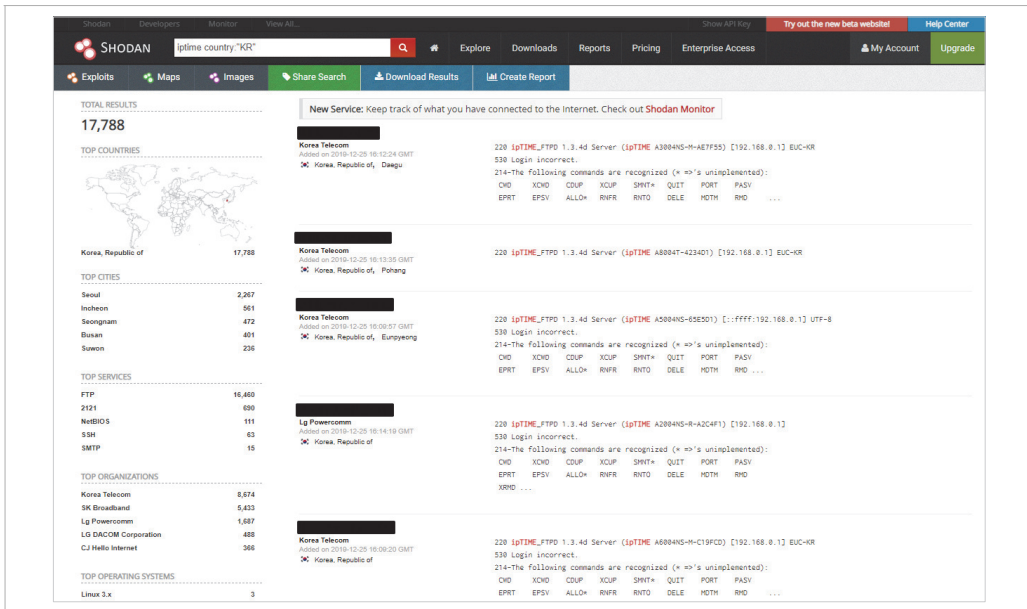
4차 산업혁명의 7대 기술 중 하나인 사물인터넷의 다양한 스마트 기기들은 이전에는 없던 사용자 경험과 다양한 정보를 제공함으로써 우리 삶의 질을 높여주고 있으며, 센서 등 산업용 사물인터넷 기기들은 에너지·물류·제조 등의 전반적인 산업에서 생산성 및 효율성을 증대시키는 역할을 하고 있다.

엄청난 양의 기기들이 네트워크에 연결되는 5G의 Massive IoT 환경에서 가장 큰 위협은 바로 보안 취약점을 내포하고 있는 기기들이다. Massive IoT 환경의 기기들은 그 유형(TV, CCTV, 시계 등)이 서로 매우 달라 공통 아키텍처나 프로토콜 설계가 어렵고, 특히 저사양의 기기들은 보안 기능 탑재 자체가 어려워 5G 시대의 대표적인 위협의 근원지가 될 수 있다.

취약한 기기들

쇼단(Shodan)이라는 검색엔진을 한번쯤은 들어봤을 것이다. 쇼단은 IP카메라, CCTV, 스마트TV·냉장고, 의료장비, 라우터 등 인터넷에 연결된 전 세계의 기기들을 검색할 수 있는 검색엔진이다. 누구나 쇼단에 접속하여 간단한 검색어만으로 인터넷에 연결된 IP 카메라나 인터넷 공유기 등을 쉽게 찾고 접속할 수 있다.

[그림] 쇼단에서 iptime을 검색한 결과



많은 기기들이 식별·인증 기능이 없거나 기본 아이디와 패스워드가 그대로 방치되어 있는 경우도 많다. 쇼단에서 검색한 IP 카메라나 인터넷 공유기에 접속하여 해당 기기가 제공하는 기본 아이디와 패스워드를 입력하여 누구나 접속이 가능하다는 의미이며, 이는 개인정보 유출이나 내부 네트워크 노출을 통한 악성코드 감염 등으로 이어지는 심각한 보안 위협이 될 수 있다.

5G와 함께 본격적으로 IoT 시대가 시작되면서 새로운 기기들이 앞 다투어 출시되고 있다. 많은 신생 업체들이 시장 선점을 위해 보안에 중점을 두기 보다는 빠른 생산 및 공급에 초점을 맞추면서 취약한 기기의 수가 늘고 있다. 소비자들 또한 스마트 기기를 구매할 때, 보안을 고려하지 않는다. 소비자에게 가장 중요한 것은 해당 기기가 제공하는 기능이나 제품의 가격이다. 가격 경쟁력이 중요한 시장에서 저비용의 기기를 생산하는 기업이 보안 기술에 집중하는 것은 정말 어려운 일이다. 또한 저전력, 저사양이라는 많은 IoT 기기들의 특성상 높은 수준의 인증이나 보안 기술을 탑재하는 것이 애초에 어렵고, 보안 취약점을 내포하고 운영되는 경우가 많아 정보유출 등의 위협에 노출되어 있다. 심지어 펌웨어 업데이트를 고려하지 않고 생산되고 판매된 기기들은 보안 취약점이 발견되어도 조치할 수가 없는 경우도 발생하며, 생산업체들의 파산으로 취약점이 해결되지 않은 기기들이 방치되는 것은 큰 골칫거리가 될 수 있다.

5G 환경에서 새롭게 출현하는 기기들의 우리의 삶과 사회 전반적으로 많은 혜택을 주는 동시에 지금까지와는 다른 더 큰 보안 위협의 잠재성을 내포하고 있다.

엄청난 규모의 DDoS 공격

2016년 10월 봇넷에 감염된 CCTV, 로봇청소기, 라우터 등의 대규모 DDoS 공격에 의해 미국의 트위터, 넷플릭스, 뉴욕타임즈, CNN 등 주요 사이트가 장시간 서비스가 중단되었으며 엄청난 피해를 입었다. 바로 미라이 봇넷 DDoS 공격이다.

봇넷은 취약점을 내포하고 있는 기기들을 감염시켜 감염자(공격자)가 목표로 하는 시스템을 다운시키거나, 대규모 스팸 전송 혹은 정보 탈취 등에 활용되는 감염된 기기인 봇(bot)들의 집합을 의미한다.

미라이 봇넷은 앞서 설명했던 것과 같이 인증이 취약한 기기들을 스캔하여 접속하고 악성코드를 감염시킨다. 감염된 기기가 주변의 또 다른 취약한 기기들 감염시키는 방식으로 빠르게 확산되었다. 미라이 봇넷은 현재도 전파되고 있으며 전 세계에 걸쳐 수십만 대의 기기들이 감염된 상태로 방치되고 있으며 간헐적으로 DDoS 공격을 감행하고 있다.

대역폭이 증가한 5G 환경에서는 봇들이 사용할 수 있는 대역폭도 증가했으며, 늘어난 대역폭은 취약한 기기를 더 많이 찾아 감염을 확산시키는데 사용될 수 있다. 초고속, 초저지연의 특성상 봇넷이 찾을 수 있는 취약한 디바이스의 수도 더 빠르게 증가하며, 소비자들 또한 스마트 홈 기기들과 같은 취약할 수도 있는 기기들을 빠르게 구매하고 있다. 그만큼 봇넷에 의한 잠재적 DDoS 공격 위협이 증대되고 있다.

미라이 봇넷 DDoS 공격은 1Tbps 규모가 넘는 엄청난 규모의 공격이었다. 하지만 5G 환경에서 악용될 가능성을 지닌 기기 수의 증가와 공격에 활용할 수 있는 대역폭의 증대는 이제까지 경험하지 못했던 훨씬 더 큰 규모의 DDoS 공격의 발생할 수 있으며 기업들은 이에 대비해야 한다.

5G 네트워크 슬라이스 간 격리 이슈

기존과 5G 네트워크의 또 다른 차이점은 망 구성에서 찾을 수 있다. 기존 네트워크 환경에서는 분야별 그리고 용도별 망 구성 시 물리적으로 분리된 폐쇄적인 구조였지만, 5G 네트워크에서는 여러 분야·용도의 망을 소프트웨어 기반의 네트워크 슬라이싱 기술을 이용하여 분리한다.

[그림] 소프트웨어 기반 기술로 다수의 망을 논리적 네트워크 슬라이스로 구성



예를 들어 모바일 네트워크 망과 자율주행, IoT 망이 하나의 물리적인 망에서 논리적인 네트워크 슬라이스(가상 전용망)로 구성되는 방식이다. 이는 네트워크 슬라이스 간 격리가 제대로 되지 않았을 경우, 하나의 슬라이스가 침해당하면 다른 슬라이스도 함께 침해될 가능성이 높다.

더 많은 보안 위협들

유럽연합 네트워크 정보보호원 (ENISA, European Union Agency for Network and Information Security)의 보고 자료에 따르면 5G 네트워크는 4G 등 이전 세대의 네트워크가 가지고 있는 취약점이 동일하게 존재한다고 경고했다. 대표적으로 SS7 & Diameter 취약점으로 네트워크 트래픽을 도청하여 SMS 메시지를 가로채거나 다른 곳으로 보낼 수 있는 취약점이다. 또한 유럽연합 네트워크 정보보호원은 'ENISA THREAT LANDSCAPE FOR 5G NETWORKS' 보고서에서 소프트웨어 기반 네트워크 아키텍처인 SDN/NFV의 취약점 등 5G 핵심 기술의 7개 영역에 대한 보안 위협을 발표했다.

5G 시대와 함께 자율주행과 증강현실(AR) 등의 기술은 더욱 발전하고, 상용화가 가속화될 것이다. 하지만 자율주행 기술이 적용된 자동차의 경우 공격자들의 표적이 되기 더 쉬우며, 취약점 등이 발견될 경우 탑승자의 생명과 직결되는 등 보안 위협에 따른 심각성이 매우 높다. 증강현실 또한 사용자의 위치를 기반으로 한 서비스가 많아 개인정보의 탈취 등의 침해사고가 발생할 가능성이 높으며, 산업현장에서 활용되는 증강현실 서비스를 공격하여 조작된 정보를 제공할 경우 큰 재난이 발생할 수 있다.

가정에서 아이의 안전을 위해 설치한 IP 카메라가 도촬용 카메라로 활용될 수 있고, 스마트 냉장고·TV·체중계 등을 통해 개인정보가 유출될 수도 있다. 공장의 기기들이 랜섬웨어에 감염되어 가동을 멈추고, 도로의 교통 시스템을 마비시켜 사고를 유발 시

키는 등 우리는 5G 시대와 함께 이전에는 경험할 수 없었던 보안 위협들에 직면할 수 있다.

5G로 인해 스마트홈, 스마트팩토리 그리고 스마트시티까지 모든 기기들이 네트워크에 연결된 사회가 눈앞에 다가왔다. 5G 시대의 사이버 공격과 위협은 그 이전과는 상할 수 없을 정도로 위력적이고 큰 테러로 이어질 수 있다.

5G 시대의 정보보안

앞서 살펴본 것과 같이 5G는 4차 산업혁명에 기반이 되는 인프라가 될 수 있고, 새로운 기술들이 나타나고 성장하는데 중요한 역할을 할 것이다. 이러한 5G 기술의 중요성과 함께 많은 전문가들은 5G 보안의 필요성을 강조하고 있다. 프라이버시 침해, 대규모 DDoS 공격, 자율주행 자동차 해킹 등 함께 다가올 보안 위협에 대한 준비가 필요하다.

5G 도입에 따른 가장 큰 변화 중 하나는 네트워크 환경의 변화이다. 클라우드 활용의 증대, SDN/NFV 소프트웨어 기반 아키텍처 등으로 5G 시대의 네트워크 환경은 더욱 복잡해졌고, 이런 복잡성 증대는 네트워크의 가시성을 확보하는데 어려움을 주고 있다. 또한 복잡한 네트워크 환경에 따라 공격의 루트가 다양해지면서 더 많은 보안 위협에 노출될 가능성이 있다. 5G에 의한 네트워크 환경 변화에 따라 네트워크 보안 시장이 확대될 것으로 예상된다. 네트워크 보안 기업들은 차세대 네트워크 보안 플랫폼을 통한 네트워크 가시성 확보와 고도화된 악성 트래픽 탐지 기술 등으로 5G 네트워크 보안 시장을 두드리고 있다. 또한 5G 인프라 확대 구성에 따른 차세대방화벽(NGFW), 침입방지시스템(IPS) 등과 같은 기존 네트워크 보안 장비 수요 확대로 네트워크 보안 시장의 전반적인 성장에 대한 기대감이 크다.

기존 보안 분야 외에도 5G 시대의 보안 트렌드로 주목받는 기술은 양자암호통신, 블록체인이 있다.

양자암호통신

1994년 피터 쇼어 박사가 양자 기술을 이용해 소인수분해 시간을 획기적으로 줄일 수 있는 알고리즘을 발표한 뒤, 기존 공개키 기반의 암호화 기술이 무력화 되는 것의 대안으로 등장한 기술이 양자암호통신이다. 양자암호통신 기술은 양자역학의 특성을 이용한 기술로 정보통신산업진흥원(NIPA)의 2018년 보고 자료에 따르면 2025년까지 글로벌 양자암호통신 기술 시장은 27조원, 국내 시장은 1.4조원까지 성장할 것으로 예상된다.

양자암호통신은 양자의 양자중첩, 양자얽힘, 불확정성 등의 특성을 이용한 기술로 양자키분배(Quantum Key Distribution, QKD) 기술에 의해 구현된다. 양자암호통

신은 양자통신을 의미하는 것이 아닌 QKD 기술로 종단 간 암호키를 안전하게 생성·분배하여 암호화 통신하는 기술이다.

양자암호통신을 위해서는 종단 간 QKD 장비 구성이 필요하며, QKD를 구성하는 주요 기술은 단일 광자 생성·검출기, 난수 발생기, 양자 암호 프로토콜, 양자 중계기 등이 있다. 양자암호통신에서는 정보의 기본 단위를 단일 광자로 사용하며, 단일 광자는 양자역학의 복제 불가능 특성에 따라 공격자에 의해 광자가 도감청 되는 것을 방지하여 보안성을 갖게 해준다. 기존 암호 기술에서 사용한 유사 난수는 초기 숫자(Seed number)가 주어지면 수학적 알고리즘을 이용해 난수를 만들어 냈다. 하지만 초기 숫자가 정해져 있었기 때문에 예측 가능하여 완벽한 난수라 할 수 없었다. QKD를 구성하는 난수 발생기는 유사 난수발생기와는 달리 수학적 알고리즘에 의존하지 않고, 물리적 임의성질에 의존하므로 예측이 불가능하고 반복 불가능한 진정한 난수를 생성할 수 있다. 양자암호통신 기술의 출현으로 기존 암호화 기술이 무의미해지는 것은 아니다. 양자암호통신은 양자의 물리적 특성을 이용하여 안전하게 비밀키를 생성하여 분배하는 기술로 암호화 데이터 전송에는 기존 암호화 기술과 기존 통신 채널을 활용한다.

양자암호통신 기술은 5G 네트워크 보안 강화에도 중요한 기술로 인식되고 있다. 국내 이동통신사들도 양자암호통신 기술의 표준화와 연구개발에 집중하고 있으며, SK텔레콤은 5G 가입자 인증 서버에 양자난수생성 기술을 적용했다고 발표했다. 하지만 모든 인프라와 기기에 양자암호통신 기술을 적용하기에는 비용적인 측면 등 아직 고려해야 할 여러 과제들이 남아있다.

블록체인

2017년 전 세계는 비트코인이라는 암호화폐의 폭등에 열광했고, 17세기 네덜란드의 튜립 파동에 비견되는 암호화폐 투기 열풍이 불었다. 블록체인은 투기 열풍을 통해 그 어떤 기술보다도 큰 인상을 주며 세상에 알려졌다. 블록체인은 1991년 처음 아이디어가 제시되었으며, 2009년 1월 3일 사카시 나카모토라는 익명의 개인 혹은 단체에 의해 비트코인이라는 암호화폐로 실현되었다.

블록체인은 완전히 새로운 기술이 아닌 기존의 기술들을 조합하고, 암호화 및 합의 알고리즘을 입히면서 탄생한 기술이다. 블록체인은 데이터 분산 처리 기술로 중앙기관·시스템 없이 생성된 데이터의 위·변조를 방지하여 무결성을 보증한다. 즉, P2P 환경에서 데이터를 거래할 수 있으며, 이 거래 기록을 안전하게 보관하고 변조가 불가능하도록 하여 보안성과 투명성을 제공한다. 또한 블록체인에 기록된 데이터를 위·변조하기 위해서는 블록체인 참여자 51%의 데이터를 동시에 해킹해야 하므로 사실상 불가능에 가깝다. 다만 블록체인에 저장된 데이터에 대한 기밀성을 제공하지 않는다. 블록체인은 트랜잭션 데이터에 대해서 네트워크에 참여할 수 있는 누구든지 저장된 데이터를 조회하고 결과를 확인할 수 있다. 이러한 투명성과 함께 블록체인은 높은 가용성을

제공할 수 있다. 기존 인프라 환경에서는 중앙 관리 시스템이 DDoS 공격으로 다운되면 어떠한 데이터도 확인이 불가능 했지만, 블록체인은 특정 참여 노드가 공격당하더라도 자신과 가까운 노드의 데이터를 확인할 수 있다.

블록체인을 다양한 분야에 적용하는 연구가 활발하게 진행되고 있으며, 보안 분야에서도 여러 시도와 많은 연구·개발이 진행 중이다. 해외에서 블록체인을 적용한 사례를 살펴보면, 독일의 자동차 제조기업 포르쉐(Porsche)는 차량의 출입문 인증 시스템에 블록체인 기술을 적용하여 기존보다 빠르고 안전한 사용자 인증을 적용하였다. 또 다른 독일 기업 보쉬(Bosch)는 차량의 GPS로 파악한 실시간 주행 거리 데이터 조작을 방지하기 위해 블록체인 기술을 적용했다. 블록체인의 특성상 보안 분야에서는 인증이나 데이터 위·변조를 방지하기 위해 많이 활용된다. 에스토니아의 보안기업 가드타임(Guardtime)은 공개키 기반 구조(PKI)를 대체하는 블록체인 솔루션을 에릭슨(Ericsson), 미육군(US Army), 록히드마틴(Lockheed Martin) 등에 제공하고 있다.

블록체인을 활용한 IoT 환경의 보안 강화 기술 연구 및 적용도 많이 진행되고 있다. 앞서 설명한 것과 같이 초연결 5G 시대에서 IoT 기기의 해킹은 큰 보안 위협으로 이어질 수 있다. 블록체인 기술을 활용하여 IoT 기기 인증이나 데이터 위·변조 방지 등의 보안을 적용할 수 있으며, 프라이버시 데이터의 부문별한 공유를 차단할 수 있다. 최근 국내 적용 사례로 KT는 5G 보안으로 기기별로 고유 ID를 부여하고, 통신 토큰이 있는 경우에만 기기 정보를 공유하는 블록체인 기술을 발표했다.

5G 기술은 더욱 우리 삶에 자연스럽게 정착할 것이고, 자율주행 기술과 같이 높은 편의성을 가져다주는 신기술들은 더욱 확산 될 것이다. 5G와 초연결 시대로의 진입, 그리고 네트워크 환경이 변화하면서 차세대(Next-Generation) 기술을 활용한 보안 기술과 플랫폼이 주목을 받을 것이다. 인공지능 기술을 활용한 차세대 보안 플랫폼들은 과도하게 탐지되는 위협 이벤트들에 대한 정확도를 높여 정교하게 위협에 대응할 수 있도록 하며, 더 나아가 알려지지 않은 위협들을 사전에 탐지하고 대응할 수 있는 기술도 출현하고 있다. 차세대 접근통제 기술은 취약한 수많은 IoT 기기들에 대한 가시성을 확보하고, 안정성이 확보되지 않은 기기·단말에 대한 접근을 사전에 차단하여 높은 보안을 유지할 수 있도록 식별·인증 기술을 연구·적용하고 있다. 또한 기존 보안 기술이 사전에 방지하던 소극적인 방식에 초점을 맞추었다면, 향후에는 MDR(Managed Detection & Response) 서비스와 같이 적극적으로 보안 위협을 탐색하고 대응하는 기술과 서비스가 부각될 것으로 예상된다. 잠시 주춤했던 보안 시장도 새로운 기술의 등장과 함께 다시 성장할 것으로 기대된다.

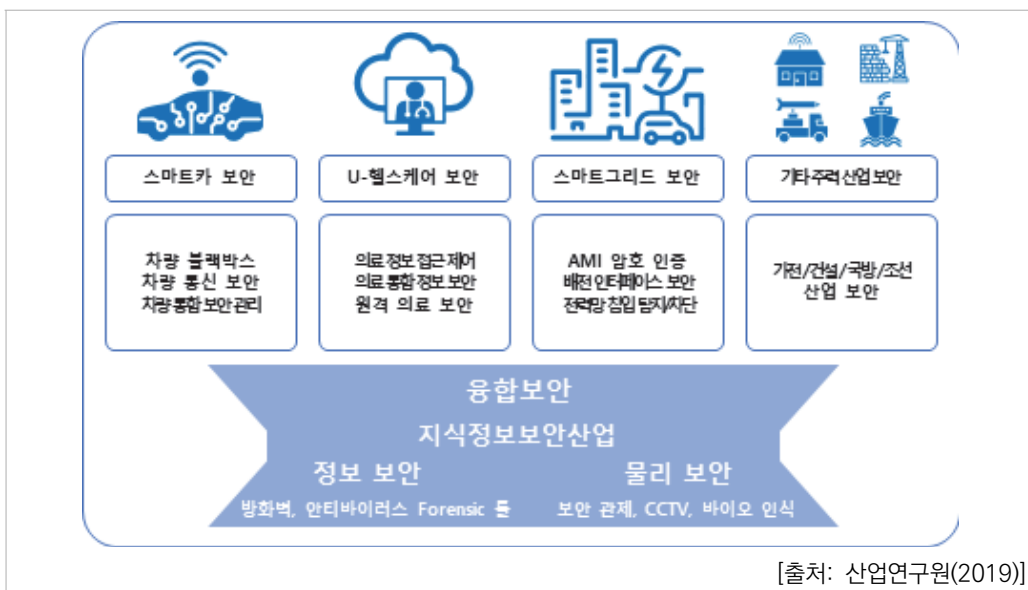
융합보안의 현황과 미래전망

중앙대학교, 장항배 교수

1. 융합보안 개념 및 범위

“융합보안(convergence security)”이란, 다양한 보안방법들의 연계 또는 통합의 의미로 사용되었으나(좁은 의미), 최근에는 ICT기술이 내재화된 융합제품(서비스)에 대한 위험을 최소화하기 위한 보안대책으로 정의된다. 따라서 ICT기술 내재화 여부와 관계없이 산업의 고유자산을 대상으로 위협대책을 수립하는 산업보안 영역의 일부분으로 정리된다(전민서, 장항배, 2019). 따라서 융합보안은 융합제품과 서비스에 대해 기획 및 설계 단계부터 보안에 대한 수립 필요성이 존재하며, 보안 사고에 대한 예방 대책과 함께 신속한 복구 등을 보장해야 한다. 기존에 회자되었던 물리보안과 정보보안에 대한 단순 결합에서 벗어나 빅데이터, 사물인터넷, 모바일 환경 등 미래 컴퓨팅 환경에서 산업특성을 고려하여 스마트 카, 의료 서비스, 스마트 공장, 스마트 홈 등에 대한 물리적, 정보보안 활동 등을 포함한다.

[그림] 융합보안 개념과 범위

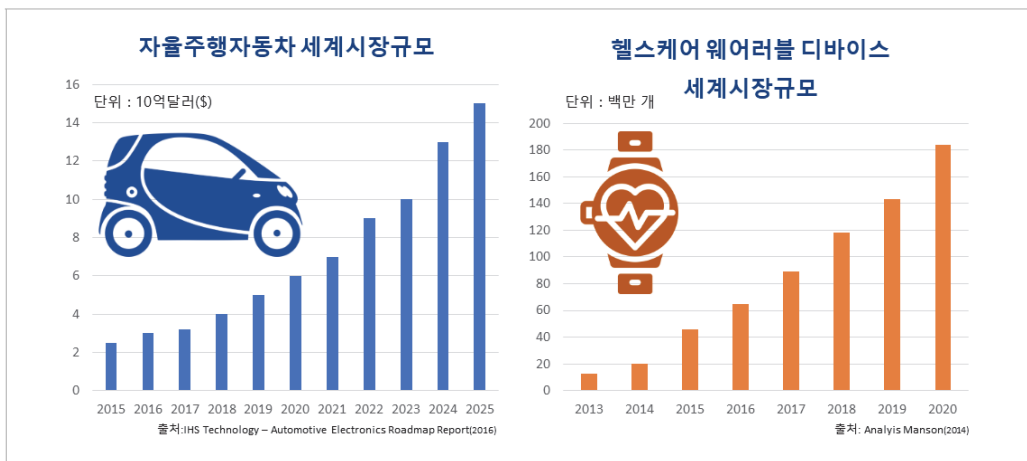


2. 융합보안 현황 및 시장전망

(1) 융합보안의 현황

산업융합 환경으로의 변화에 따라 기존 제품이 스마트 기술과 융합되어 다양한 형태로 변화되고 있다. 제품의 경우, 기존 제품에 스마트 기술을 내재화하여 자율주행자동차, 스마트 선박, 헬스케어 웨어러블 기기 등 새로운 형태와 기능을 보유한 제품 생산이 진행되고 있으며, 시장 규모 또한 증가하고 있다. 또한 스마트 기술이 융합된 서비스가 발전하면서, 실제 제조 산업을 중심으로 스마트 팩토리가 등장하여 설계·개발, 제조 및 유통·물류 등의 생산 과정 전체에 스마트 기술이 접목되면서 공정의 생산성, 품질, 고객만족도를 향상하는 지능형 생산공장이 출현하고 있다. 가정환경에서도 TV, 냉장고, 세탁기 등 집안의 다양한 기기들이 네트워크에 연결되어 지능형 서비스를 제공하는 스마트홈이 등장하여 편의성을 제공하고 있다.

[그림] 산업융합 제품의 세계 시장규모



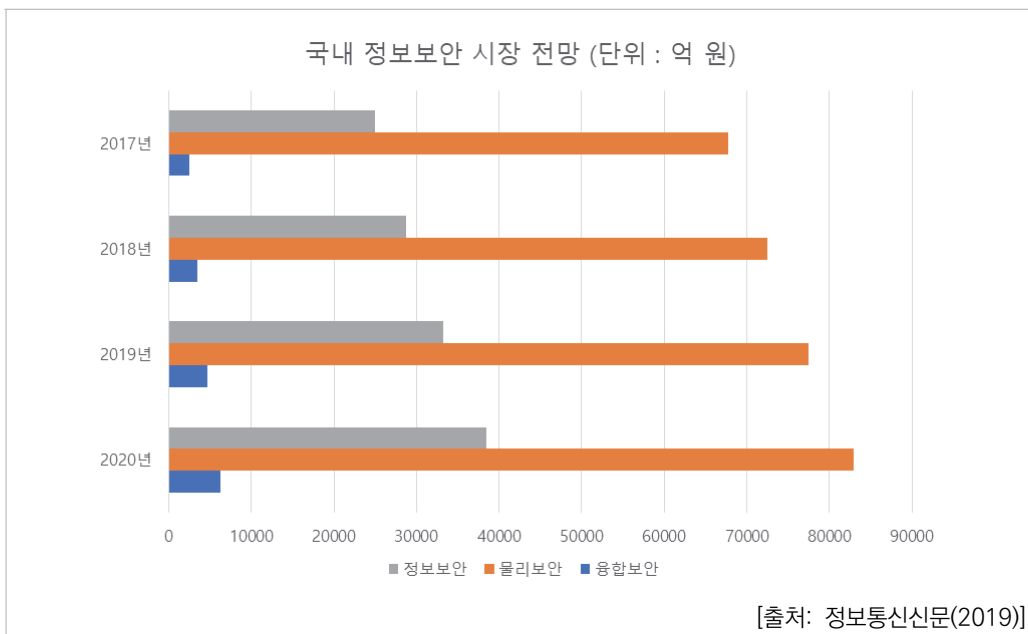
(2) 융합보안 시장전망

융합보안은 4차 산업혁명 시대의 ICT사회에서 더욱 중요한 산업이 될 것이다. 더하여 빅 데이터와 인공지능 등의 기술체제와 인프라에 대한 공격도 증가할 것으로 예상된다. 따라서 보안의 대상이 컴퓨터나 모바일 기기 등 내부 네트워크 중심에서 대표적인 ICT 기술인 인프라 시스템에 대한 보안으로 범위가 확장된다.

글로벌 IT 리서치 기업인 가트너(Gartner)는 2018년 8월 발표에서 국내 보안 시장은 지난해 대비 올해 9.4% 증가한 2조 2000억원 규모에 육박할 것으로 전망했다. 특히 보안 서비스 부문이 1조 2600억원 규모로 전체 시장의 절반을 넘어서고, 이 중 가

장 작은 규모인 클라우드 보안이 4차 산업혁명의 도래에 따라서 가장 빠른 성장세를 보일 것으로 예측했다. 융합보안의 경우는 현재의 시장규모 자체는 작은 편이지만 정보보호 산업에서 가장 큰 성장률을 기록하여 향후 유망 분야로 예상된다고 밝혔다. 또한 한국전자통신연구원(ETRI)은 글로벌 보안 시장이 2020년에는 2392억 달러 규모로 성장할 것으로 내다봤다. 한국전자통신연구원은 세계 정보보호시장이 2020년까지 융합보안시장이 34.3%의 연평균 성장세를 이어 갈 것으로 분석하고, 4차 산업혁명의 발전에 따라 정보보호 산업 부문 중 가장 큰 성장률을 기록하여 향후 유망 산업분야로 예상된다고 예상했다. 또한 정보보안 제품시장은 상대적으로 진입장벽이 낮아서 미래의 시장 가치가 높을 것으로 예상되는 보안 SW와 가상사설망·방화벽의 시장 진입 노력이 요구되며 특히 4차 산업혁명의 발전과 함께 클라우드, 사물인터넷 등 급변하는 네트워크 인프라 환경에 따른 네트워크 장비에서 통합적 보안기능을 제공할 수 있는 전략이 필요할 것으로 전망된다고 분석했다.

[그림] 국내 정보보안 시장 전망

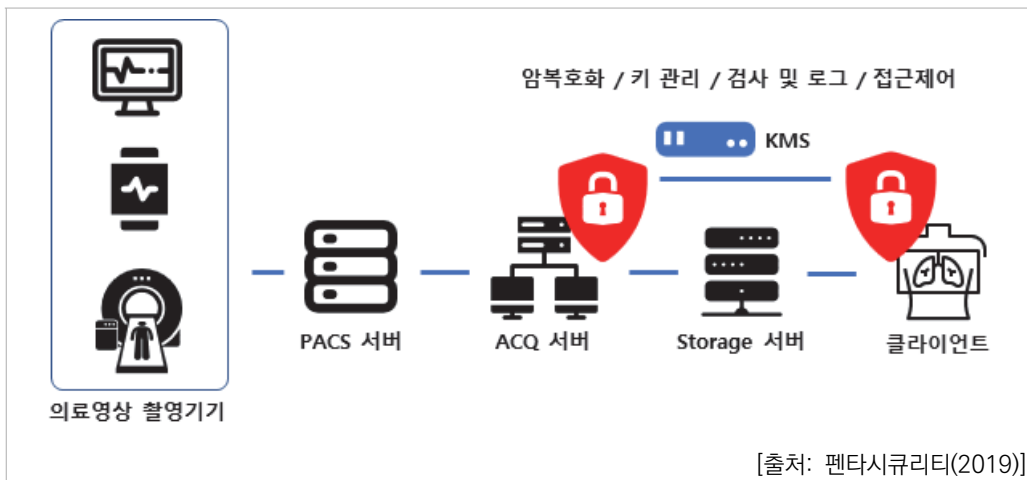


3. 산업융합보안 사례

(1) 의료정보 보안

의료정보란 의료 제공의 필요성을 판단하기 위하여 그리고 의료행위를 통하여 수집된 자료를 기초로 하여 연구 및 분석된 정보들을 포괄하는 것이다. 또한 이는 진단과 치료, 치료 후의 관찰 등을 포함하여 의료행위를 통한 과정에서 수집된 환자의 건강상태에 관한 정보이다. 특히 의료 기관에서는 진료신청과정, 진료과정, 처방과정에서 환자의 개인정보 및 민감정보를 다수 수집한다. 바이오정보, 비밀번호, 고유 식별정보 등과 같은 주요 개인정보는 암호화 등의 안전한 보호조치를 통하여 개인정보처리시스템에 저장되거나 네트워크를 통하여 전송되어야 한다. 고유식별정보와 비밀번호, 바이오정보는 암호화 대상 개인정보이다. 의료 ICT와 결합된 의료영상저장전송시스템(Picture Archiving and Communication System)은 디지털에서의 의료영상 이미지를 저장, 가공 및 전송하는 통합 관리 시스템을 말한다. 이 시스템에서 전송되는 의료영상 이미지는 환자의 민감한 정보이기 때문에 외부에 유출되지 않도록 안전하게 관리되어야 하며, 이 시스템을 전송되는 데이터를 암호화하여 공격자로부터 의료영상 데이터를 안전하게 보호해야 한다.

[그림] 의료정보 보안



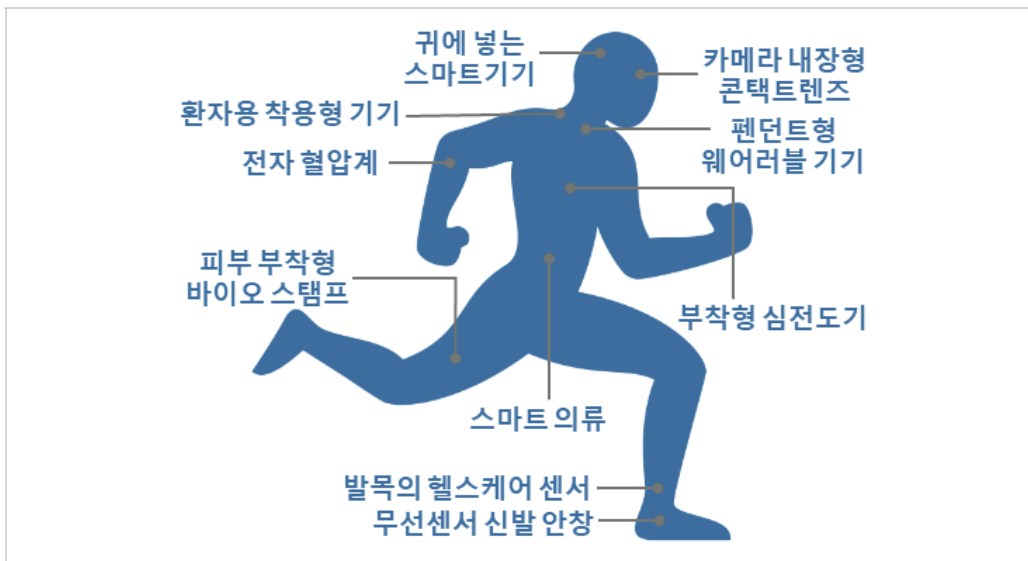
(2) 헬스케어 웨어러블 기기 보안

헬스케어 보안 분야는 의료기기에 대한 침해 방지와 스마트 의료보안 플랫폼 등을 중심으로 개발되고 있다. 의료기기 침해방지기술 분야에서는 헬스케어와 의료기기 및 게이트웨이에서의 보안 취약성을 탐지하고 이를 차단하기 위한 기술이 개발되고 있다.

미국 매사추세츠 대학에서는 의료 기기에서의 악성코드 탐지 기술을 포함한 60여개 이상의 헬스케어 보안 기술 개발이 진행 중이다. 에리조나주립대에서는 생리정보를 이용하여 의료기기 인증 기술과 암호 프로토콜을 개발하는 등 헬스케어 보안에 대한 기술이 세계적으로 개발되고 있다.

국내에서는 의료 데이터의 안전한 전송을 위한 보안 프로토콜 기술 개발과 헬스케어, 의료기기에 대한 사용자 인증에 집중하고 있다. 의료정보 보안 기술 분야는 의료 데이터를 분석하여 개인에 대한 식별화 공격에 대한 지능적인 방어 시스템과 데이터 트러스트 분석 기술을 활용하여 의료정보에 대한 프라이버시와 무결성을 보장하는 연구가 진행 중이다.

[그림] 헬스케어 보안



(3) 자율주행 자동차 보안

자율주행 자동차는 운전자의 조작 없이 자동차가 스스로 운행을 할 수 있는 자동차를 말한다. 이는 고성능 카메라, 충돌 방지 장치 등의 기술적 발전이 필요할 뿐만 아니라 주변 주행상황의 정보를 종합하여 판단 후 처리하는 주행상황에 대한 인지 및 대응 기술이 필수적이다. 현재의 자율주행 자동차의 기술발전 상황은 다음 <표 00>에서의 2~3단계에 해당한다.

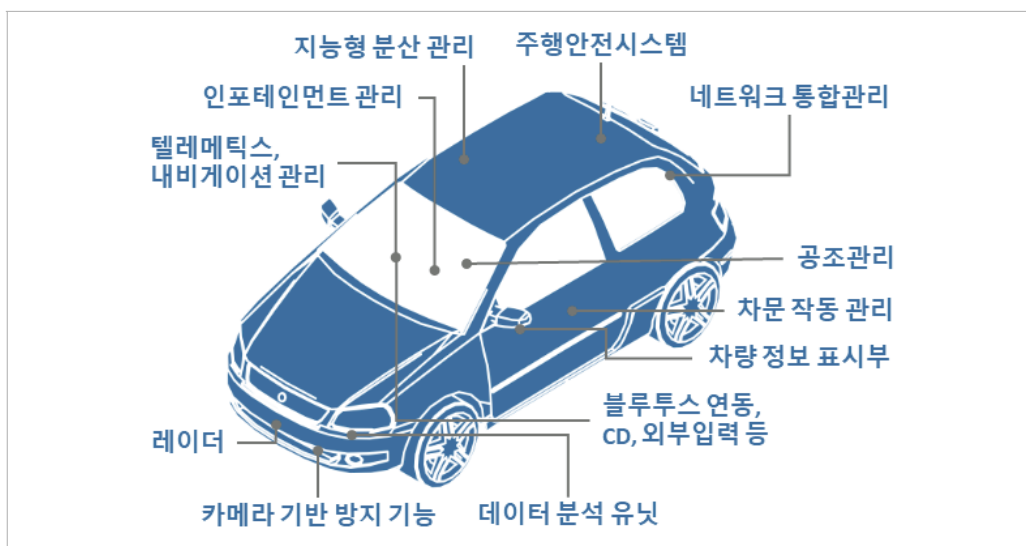
[표] 미국자동차공학회 자율 주행 단계

단계	기능	설명
1	단일 주행 보조기능	- 단일 기능의 운전자 보조 시스템 활용 - 크루즈 컨트롤, 차선유지 등 - 운전자가 직접 운전
2	복수 주행 기능 융합 보조	- 2개 이상의 주행기능이 융합 보조 - 차선유지, 적응형 크루즈 컨트롤 등 - 운전자는 주행상황 항상 주시
3	제한된 자율주행	- 특정 도로 조건에서 제한된 자율주행 - 고속도로 자율 주행 등 - 운전자는 위기상황시 개입
4	완전 자율주행	- 모든 도로 조건에서 자동 제어 - 운전자 탑승
5	무인 완전 자율주행	- 모든 도로 조건에서 자동 제어 - 무인 운전

[출처 : Electronics and Telecommunications Trends(2018)]

자율주행자동차에 있어서 가장 큰 보안 문제는 차량 내부 네트워크의 위·변조 등의 내부네트워크 보안 문제와 무선 통신망 해킹, Dos 공격을 통해 외부네트워크에 대한 보안문제가 존재한다는 것이다. 이에 현재 자율형차량 보안을 위해 침입탐지 시스템 (IDS), 차량용 방화벽(F/W) 등의 ICT 보안 기술들이 개발되고 있다.

[그림] 자율주행차량 보안



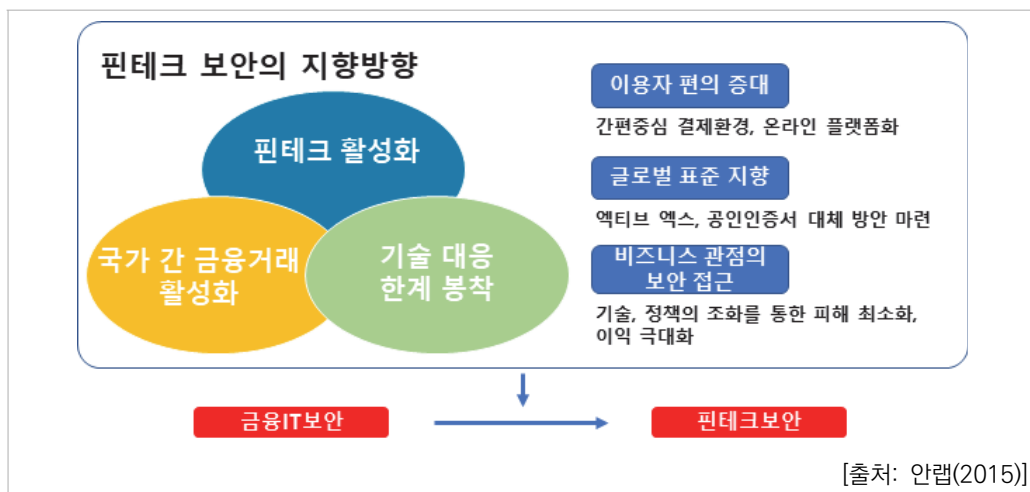
(4) 금융(핀테크) 보안

핀테크 서비스는 P2P영역에서의 결제와 송금 시스템, 금융 데이터 서비스, 카카오프뱅크 등의 인터넷 은행, 가상화폐, 클라우드 펀딩 등 온라인과 오프라인을 초월한 금융 서비스이다. 이는 금융 분야에서 이용자 편의를 혁신적으로 발전시켰지만 다양한 보안 위협이 있다.

핀테크는 금융·IT 기술융합·기술 발전에 따른 이용자 편의성 중심의 서비스 출시, 새로운 기술 도입에 따라 신규 보안 취약점이 생겨나고, 이를 통해 보안 사고의 발생 가능성이 증가한다는 것이다. 기존에는 사용자와 거래내역 인증을 위해 단말 플랫폼 보안, 공인인증서, 추가 인증 수단 등을 사용하였지만 핀테크의 발달을 통해 결제단계를 생략하는 등 절차를 줄이는 과정에서 보안 취약점이 발생할 수 있다. 또한 개인 금융 정보 공유 채널의 확산에 따른 정보 유출의 가능성이 발생할 수 있다. 관리 대상의 증가로 금융기관 간의 책임 영역이 모호해질 수도 있으며 연계 및 제휴되어있는 금융 시스템 전체로 보안 사고의 확장이 쉬워질 수 있다. 마지막으로 규제 완화로 인해 금융보안 규제가 사전규제 방식에서 기업의 자율적 보안관리체계로 전환되며 보안 관리 체계에 대한 대처가 미흡한 기업을 통해 보안 사고가 발생할 수 있다.

이에 대한 대응방안으로는 사용자 인증 기술에 보안성이 확보될 수 있어야 하며, 단말에 대한 보안 방안 수립하여야 하고 새로운 기술에 대한 보안 취약점 진단 체계를 수립하여야 한다. 또한 시나리오 방식의 보안 위협 체크리스트 작성과 기관 간 연계 구간에 대한 데이터 보안 방식을 확정하고, 사기거래 탐지 고도화를 통한 모니터링 체계를 강화하여야 하며, 핀테크 산업 육성을 위한 정부 지원체계를 수립하여야 한다.

[그림] 핀테크 보안

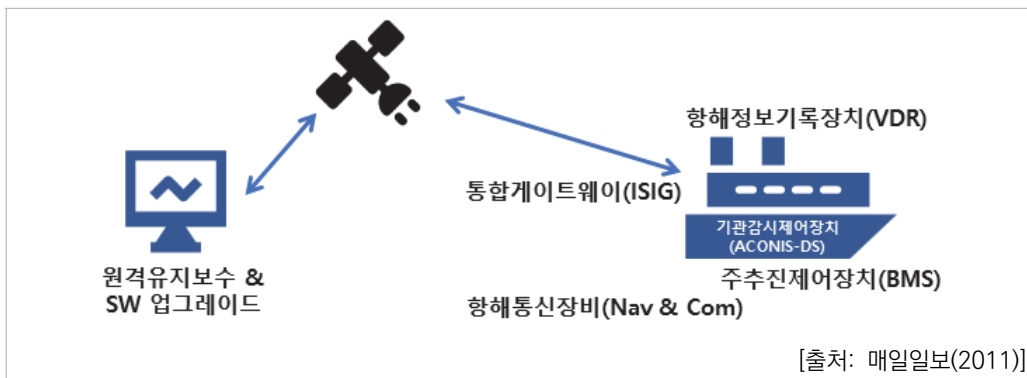


(5) 선박(지능형선박 보안)

선박 분야에서는 해양수산부가 구축하고 있는 해상 전용 LTE 통신망(LTE-M)과 자율주행 선박(스마트쉽)에 대한 연구 및 개발이 진행되고 있다. 시장조사업체 마켓앤마켓에 따르면 2017년 55억1000만 달러였던 '커넥티드 선박'(Connected Ship) 시장규모는 2023년까지 연평균 3.95% 성장해 71억9000만 달러에 이를 전망이다.

지능형선박의 발전에 해킹 위험 또한 증가할 것으로 예상된다. 통신망을 연결할 수 있는 커넥티드 제품은 지능형 자동차와 항공기의 경우 사이버 침입이 발생할 경우 인명과 재산 피해가 예상되고 신뢰성을 잃을 수 있기 때문에 이미 방화벽 등 사이버 보안 기술에 대한 기술 개발과 기술 적용이 활발하다. 이에 미국 국립표준기술연구소(NIST)와 국제표준화기구(ISO) 등의 주요 기관은 지능형 차량, 선박 등에 대한 표준을 제정하기도 했다.

[그림] 지능형 선박



(6) 제조(스마트팩토리) 보안

스마트팩토리란 설계, 개발, 제조, 유통, 물류에서의 생산과정과 공장 디지털 자동화 체계를 융합한 신개념의 공장을 의미한다. 스마트팩토리는 외부와의 통신을 기본으로 하기 때문에 기존 발전소나 공장 등 보다는 보다 차별화된 보안이 필요하다. 이러한 스마트팩토리 보안을 위해서는 기술적(사이버) 보안과 물리적(사람) 보안이 둘 다 중요하다.

스마트팩토리 보안이 초기 단계에서부터 사이버, 물리적 보안이 융합되어 진행되어야 하는 이유는 외부에서의 공격때문에 생산이 멈춘다면 피해가 커지기 때문이다. 스마트팩토리 보안은 단순히 돈이나 사람, 고가의 장비뿐만 아니라 솔루션을 포함한 모니터링 시스템까지도 아우르는 전체적인 융합보안이 필요한 분야이다.

[그림] 스마트팩토리

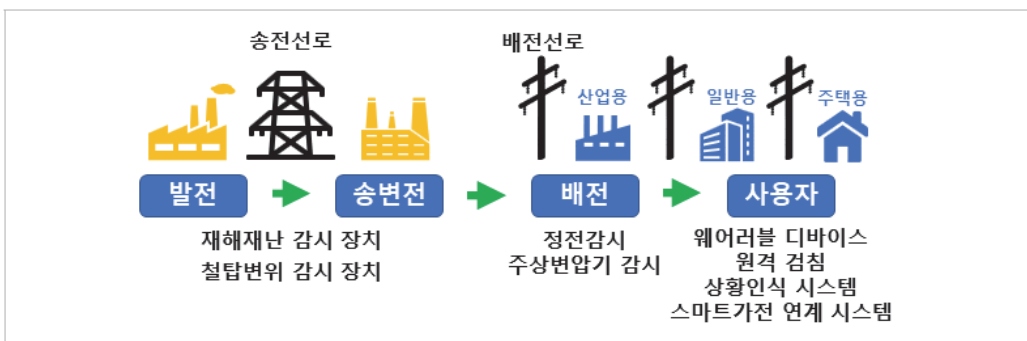


(7) 스마트 그리드 보안

스마트그리드(Smart Grid, 지능형전력망)은 기존의 발전, 송전, 배전, 판매의 단계로 구성된 전력망에 ICT기술이 결합된 지능형 전력기술이다. 이는 에너지 공급자와 소비자가 실시간으로 에너지의 사용정보를 공유하여 에너지를 효율적으로 소비할 수 있게 한다. 스마트그리드는 소비자의 편리성과 정보의 신뢰성, 무결성을 높여줄 뿐만 아니라 전력 공급의 안정성을 가져다 주며, 효율적인 에너지 관리를 통하여 에너지를 효율적으로 분배할 수 있고, 이에 따른 에너지 절감으로 저탄소 국가를 실현할 수 있다.

하지만 스마트그리드는 ICT와의 결합을 통해 개방형 전력망이기 때문에 사이버 공격 등 외부 공격에 취약하다. 스마트그리드는 소비자 편의를 위해 수요반응(DR), 지능형 검침(AMI) 등 소비자 편의성을 증시하고 전력사용의 효율성을 높이기 위해 정보 교환이 증가하기 때문에 사이버 공격의 위협 가능성이 높아진다. 특히 그 특성상 제어 시스템 위협, 네트워크 위협, 소비자 보안 위협 등의 융합적 위협이 동반될 수밖에 없다. 스마트그리드 보안은 이에 따라 스마트그리드에 특화된 보안체계가 구축되어야 하며 기술적, 법적, 제도적 보안 대책 또한 필요하다.

[그림] 스마트 그리드



4. 융합보안 향후과제

(1) 융합보안 산업 경쟁력 강화

① 융합보안 전문 기업 육성

융합보안은 지속적으로 발전하고 있지만 이에 대한 특화기업 설립과 신규창업 등의 활성화는 여전히 미흡하다. 융합보안 시장은 타 산업과 결합되는 경우가 많아서 인지도 높은 기업에게 유리하여 진입장벽이 높다. 이에 따라 세계적인 정보보호 업계에서는 융합보안 시장을 선점하기 위해 기업 간 인수합병을 활발히 추진하고 있지만, 국내에서는 아직 소극적인 상황이다.

[표] 국내·외 정보보호 분야 주요 인수합병 사례

해외 사례	인수합병 내용
IBM	키로그·애플리케이션 변조 탐지기술 등을 보유한 Trusteer를 약 10억달러에 인수하여 자체 악성코드 대응능력 확보
페이팔(Paypal)	사이버공격 위협을 사전에 예측하고 사고를 방지하는 지능형 보안 관련 기업인 사이액티브(CyActive) 인수
Rambus	스마트카드 등 디바이스 키유출 위협 분석 관련 원천 기술을 보유한 CRI를 인수하여 사물 디바이스 보안 기술력을 확보
FireEye	시큐리티 인텔리전스 역량 확보를 위해 아이사이트 파트너스 및 인보타스인수
인텔	McAfee를 인수하고, 업계최초로 CPU내 정보보호 기능을 탑재한 제품출시
블루코트	클라우드 데이터보안 솔루션 전문기업인 퍼스펙시스를 인수
국내 사례	인수합병 내용
NHN	DB보안 전문기업인 피애피시큐어 인수
엑셈	DB보안 전문기업인 신시웨이 인수

[출처: 대한민국 정부(2016)]

이에 융합보안 전문기업 설립을 유도하기 위해 융합보안 관련 기업을 대상으로 한 인수합병 등 전략적 합병을 지원하여 관련 기업의 경쟁력 강화를 도모하는 방법에 제시된다. 또한 융합보안에 관련된 기술을 보유한 개인과 기업의 창업 및 성장을 지원하기 위해 스타트업 지원도 추진하는 방법도 있다. 덧붙여 지역별로 ICT 융합산업에 특화된 보안기술 발전 지원을 위해 송파 및 판교 클러스터와 같은 지역별 융합보안 클러스터를 구축하는 방법이 있다. 마지막으로 체계적 지원을 위해 해외 전략거점 구축하고 민관이 합동하여 해외수주를 추진하는 등 글로벌 융합보안 수주동향 등이 제공되면 경쟁력 강화를 이끌어낼 수 있을 것이다.

② 융합보안 전문 인력 양성

융합보안 분야 인력수요가 증가하고 있음에도 불구하고 체계적 인력양성이 미흡하고 수요 맞춤형 인력공급이 부족한 실태이다. 융합보안 분야에 진출할 계획이 없는 기업들의 사유를 조사했을 때“전문 인력이 부족하다”는 의견이 21.9%로 2위를 차지하였다(1위는 시장성 불확실, 31.3%). 또한, 융합보안 사업 진출이 예정된 기업인데도 해당 인력을 보유하지 않은 기업이 50.7%에 달하는 것으로 조사되었다(IoT 정보보호 산업 및 기업 실태조사, 한국인터넷진흥원, '15). 이에 ICT 융합산업과 정보보호 분야에서 전문적인 지식을 모두 보유한 융합보안 전문 인재 양성을 추진해야 한다. 융합보안 분야 특성화고등학교나 마이스터고 지정을 통하여 산업과 SW, 정보보호 분야가 융합된 기본교육을 추진하고, 융합보안대학원 설립을 통해 융합보안 분야 시장을 넓혀나가야 한다.

(2) 융합보안 제도 정비

융합보안에 관한 법규와 제도를 정비하여 정보 보호를 기존 정보통신서비스를 초월하여 IoT 제품과 서비스까지 확대하는 등의 제도정비를 검토해야한다. 정부는 5G 융합제품과 서비스 보안 강화를 위한 정보통신망법 개정을 추진하고 있으며, 보안업계를 비롯한 한국인터넷진흥원의 융합보안 대책 마련이 시급하다는 요청에 따라 IoT 기기와 서비스 보안과 관련한 법적근거를 마련하는 중이다. 이에 대한 주요 내용은 아래와 같다.

[표] 5G 초 연결 환경에 대응하는 사이버보안 예방체계 확립

구 분	주요 추진내용
관리체계 강화	• 5G 네트워크 핵심시설을 주요 정보통신기반시설로 확대 지정·관리 • 주요 5G 통신서비스·융합서비스 정보보호관리체계 인증 실시
중소기업 안전	• 중소기업 현장 정보보호컨설팅 확대('18년 195건 → '20년 300건) • IoT 제품 보안 취약점 점검 지원 확대 ('18년 105개 → '20년 200개)
융합보안 제도	• 5G 융합제품·서비스에 대한 보안 강화를 위해 정보통신망법 개정 추진

[출처: 디지털데일리(2019)]

또한 주요 5G 통신서비스, 융합서비스에 대한 정보보호관리체계인증(ISMS)도 실시한다. 예를 들어 스마트공장의 경우, 일정 규모의 공장에서는 ISMS 인증을 의무화할 수 있도록 제도 및 법률을 마련할 계획이다. 또한 5G 관리체계 강화를 위해 네트워크 핵심시설을 주요 정보통신 기반시설로 확대하여 지정하고 관리할 예정이다. 또한 정보통신기반보호법에 따라 중요 정보통신 시설을 확대 지정하고 이를 집중적으로 관리한

다. 이러한 정부의 계획은 5G 시설을 확대하여 주요 기반 시설의 사이버 공격을 방어하려는 취지로 풀이된다.

참고문헌

- 전민서, 장항배, “ICT기반 보안개념 정의와 범위에 관한 설계연구”, Information Systems Review, 제21권 3호, 2019
- Economic Review, “사물 인터넷 해킹당하면 괴물 인터넷”, 2014
- 에너지경제, “이통3사 주총 개막, 핵심 키워드 IoT·배당”, 2016
- 정보통신신문, “올해 국내 보안시장 10% 성장, 공공기관 이어 민간수요 늘 듯”, 2019
- 한국정보보호산업협회, “융합보안산업 시장전망 및 경쟁력강화 방안 연구”, 2016
- The Science Times, “2020년 보안 정책의 핵심은 융합”, 2019
- 바이라인 네트워크, “문재인 정부 첫 ‘민간 정보보호 종합계획’ 마련, 융합보안이 핵심 키워드”, 2019
- 대한민국 정부, “ICT 융합 안심사회 구현 및 정보보호 신산업 육성을 위한 K-ICT 융합보안 발전 전략(안)”, 2016
- 디지털데일리, “정부 5G 플러스 전략 속 정보보안, 제도정비·산업육성 눈길”, 2019
- 권혁찬, 이석준, 최중용, 정병호, 이상우, 나중찬, “자율주행 자동차 보안기술 동향”, Electronics and Telecommunications Trends, 2018

얼굴인식시스템 동향 및 전망

슈프리마, 전동훈 수석

인터넷 사회, 개방적 정보화 사회 등으로 불리는 현대 사회에서 보다 안정되고 신뢰성 있는 사용자 확인은 필수적이다. 신뢰할 수 있는 사용자 인증은 단순한 네트워크 로그인을 하는 데 필요한 것만은 아니다. 일상의 많은 보안 사항들이 보다 강화되고, 안전하고 정확한 신분확인 은 필수적인 작업으로 여겨지고 있다.

개인이 정보 보안을 위해 가장 간편하게 할 수 있는 것은 비밀번호 방식이다. 하지만 동일한 비밀번호를 사용할 경우 해킹에 노출될 확률이 높고, 주요 사이트에서 개인 정보 유출 사건을 여러 번 겪으면서 주기적인 비밀번호 변경과 함께 비밀번호 조합 조건을 특수문자와 알파벳 대소문자 혼합 등 좀 더 복잡한 형태로 변경되었다. 이에 따라 사이트마다 다른 조건의 비밀번호 설정 때문에 사용자들이 비밀번호를 기억하는데 더 어려움이 커졌지만, 비밀번호 방식 자체가 단순하고, 이미 비밀번호를 찾는 데 필요한 개인정보가 많이 유출됐기 때문에 복잡해진 비밀번호의 보안성은 높지 않다고 판단된다.

따라서 금융 등 다양한 서비스 분야에서는 기존 방식의 위험을 인지하고 보안성을 높이기 위해 여러 가지 방법을 고민하고 적용해 왔다. 결국 기존 방식의 문제점인 복제가 거의 불가능하고, 분실의 위험이 없으며, 보안성이 높은 새로운 인증방식에 대한 수요가 커지고 있으며, 이에 현재로서 가장 적절하다고 평가되는 것이 바로 바이오정보를 이용한 바이오인식 기술이다. 바이오인식은 다른 사람이 복제하거나 대신 사용할 수 없다는 바이오정보의 특성 때문에 본인 확인에 있어서 다른 보안 방식보다 높은 신뢰성을 가지므로 다양한 서비스에 사용하기에 매우 적합한 방식이다.

바이오인식 기술은 개인 신분을 증명하는 가장 유망한 기술로 경찰청의 범죄 수사 등에 국한되어 있던 과거에서 최근 산업화가 되고 있는 기술이며, 가트너 그룹 등에서 21세기 유망 20대 기술 중 하나로 선정되었다.

또한 국제민간항공기구(ICAO)의 권고의 따라 바이오인식 기반 출입국관리시스템을 적용하여 테러용의자 조기 검거 등의 용도에서 시작하여 본인을 확인하는 서비스로 사용이 점차 확대되고 있다. 전자주민증 및 운전면허증과 같은 ID카드 발급 시 바이오정보를 이용한 신원확인으로 ID의 범죄 관련 활동을 사전에 방지하는 등 국가안전과 관련된 사업이 활발하게 진행되고 있다. 바이오인식 발전 방향이 출입통제, 네트워크 인

프라 등 주요 시스템에 대한 접근통제에서 본인 확인 수단과 스마트기기 등과의 연계를 통한 모바일 결제시스템까지 확대되고 있다.

신체적 특징을 이용한 바이오인식 기술에는 대표적으로 지문, 얼굴, 홍채인식 등이 있다. 이 중 최근에 가장 주목받고 있는 기술이 바로 얼굴인식 혹은 안면인식 분야이다. 얼굴인식은 피부색과 얼굴을 구성하는 눈, 코, 입 등의 요소 위치, 모양 등의 얼굴의 특성을 이용하여 사람의 신원을 인식하는 방법이다. 그리고 얼굴의 특성을 이용하는 방법 외에도 열화상 카메라 등을 이용하여 사람 얼굴의 고유한 열 분포 패턴을 촬영하고 이를 이용하여 인증하는 방식도 존재한다.

얼굴인식 기술은 인간이 다른 사람을 인지할 때 가장 많이 사용하는 것이 얼굴이기 때문에 가장 자연스러운 바이오인식 기술이라고 할 수 있다. 주요 활용 분야는 얼굴인식을 통한 고객 맞춤형 정보 제공(마케팅), 거짓말 탐지, 범죄 용의자 탐지(휴대용 단말기를 이용한 범죄 용의자 단속), 보안인증, 엔터테인먼트(낯은 사람 찾기), 인물 사진 관리 지원, 줄음운전 방지 등 다양한 분야로 사용처가 넓어지고 있다.

얼굴로 신원을 확인하기 위해서는 빠른 속도로 정확하게 얼굴 영역 및 얼굴의 구성요소를 검출하는 것이 필요하다. 취득된 얼굴 영역 영상은 밝기 보정, 회전 보정, 잡음 제거 등을 거쳐 최대한 일정한 형태의 영상로 변환되고 이후 눈·코·입의 위치, 비율, 크기 등 다양한 요소의 비교를 통하여 본인 여부를 확인하게 된다.

일반적인 얼굴인식 기술의 장점은 사용자가 카메라를 이용하는 거부감이 적으며, 판독을 위해 자연스럽게 제출한 사진이 남기 때문에 사용자의 사후 추적 등이 가능하다. 반면에 조명 및 환경과 영상의 각도에 민감하며, 변장, 세월이 흐르면서 생기는 얼굴 변화, 성형수술, 쌍둥이의 유사한 얼굴 특징 등을 구분하는 데 단점이 있다고 알려져 있다.

이러한 2차원 영상을 기본으로 하는 얼굴인식 기술은 같은 인물이라 할지라도 주변 환경과 표정, 머리 모양, 화장, 조명 등에 따라서 특징점의 변화가 비교적 크고, 전체적인 얼굴의 구성이 비슷한 사람들이 많이 존재하기 때문에 인식 정확도가 떨어지는 문제점을 피사체를 향해 발사한 빛이 튕겨 돌아오는 시간으로 거리를 계산하여 사물의 입체감과 공간 정보, 움직임 등을 인식하는 TOF(Time Of Flight) 기술 등과 같이 다양한 3차원 영상을 취득하는 방법으로 개선을 시도하고 있다.

또한 얼굴인식의 경우 지문인식 등 기존의 여타 바이오인식 기술보다 취득되는 영상에 영향을 미치는 환경적 요소가 매우 다양하여 취득된 영상을 비슷한 형태로 변환하는 전처리 과정에 많은 자원과 시간이 소모되고, 인식 정확도 역시 비교적 낮아 널리 보급되지는 않고 있었던 기술적 한계를 최근 딥러닝과 같은 혁신적인 기술 방법이

적용되면서 공공, 금융, 유통 등 다양한 분야에서 적용한 사례가 급속도로 증가하고 있다.

사용의 편리성과 빠른 속도, 일반인들의 거부감이 적다는 측면에서 기존 출입통제 같은 환경 외에도 특히 공항 등에서 최적의 솔루션으로 주목받고 있으며 다음과 같이 주요 적용사례가 증가하고 있다.

공항에서의 얼굴인식 기술 적용사례

- 중국은 2015년부터 정부 주도하에 13억 중국 인구의 얼굴을 3초 안에 90%의 정확도로 식별할 수 있는 데이터베이스를 구축하고 중국 전역에 얼굴인식 기능이 탑재된 카메라를 1억 대 이상 설치 운영
- 미국 뉴욕시에는 테러범 포착을 위해 모든 다리와 터널에 운전자의 신원을 확인할 수 있는 얼굴인식 카메라를 설치
- 중국 상하이 홍차오 공항의 국내선 청사는 얼굴인식 기반의 무인 출입심사 시스템 운영 중이고, 2019년 10월 개항한 베이징 신공항은 얼굴인식만으로 출입국 심사 등을 진행
- 미국 국토안보부는 1조 원의 예산을 들여, 비자 기간 초과 등을 확인하기 위해 외국 비행기에 탑승한 승객들에 대한 얼굴인식검사 도입을 추진 중
- 2018년 12월에 델타항공은 미국 관세국경보호청, 애틀랜타 국제공항, 미 교통안전국과의 협업을 통해 애틀랜타 국제공항에서 첫 번째 바이오인식 터미널을 선보임
- 싱가포르 창이공항은 비행기 탑승 시간에도 도착하지 않는 승객을 카메라로 식별하여 공항 내 탑승객 서비스 이용도를 높이기 위해 얼굴인식 시스템을 테스트 중
- 인천공항공사 2020년부터 여권·탑승권 대신 지문·얼굴 인식만으로 출국하는 시스템 도입 검토 중
- 무인상점 Amazon Go에서는 얼굴인식 기술을 이용하여 고객의 얼굴과 아마존 ID를 매칭, 해당 고객의 동선과 물품 구매 성향 등을 파악
- 중국 최대 가전유통업체인 쑤니원상의 일부 매장에서는 얼굴인식 기반의 결제서비스 제공
- 알리바바, 장둥닷컴, 빙고박스 등의 무인 매장에서 얼굴인식으로 결제 가능
- 국내 편의점 중 일부 무인 매장에서는 사전에 등록된 얼굴 정보를 활용하여 결제서비스를 시범운영 중
- HSBC은행에서 얼굴인식을 통한 계좌개설이 가능한 앱 출시

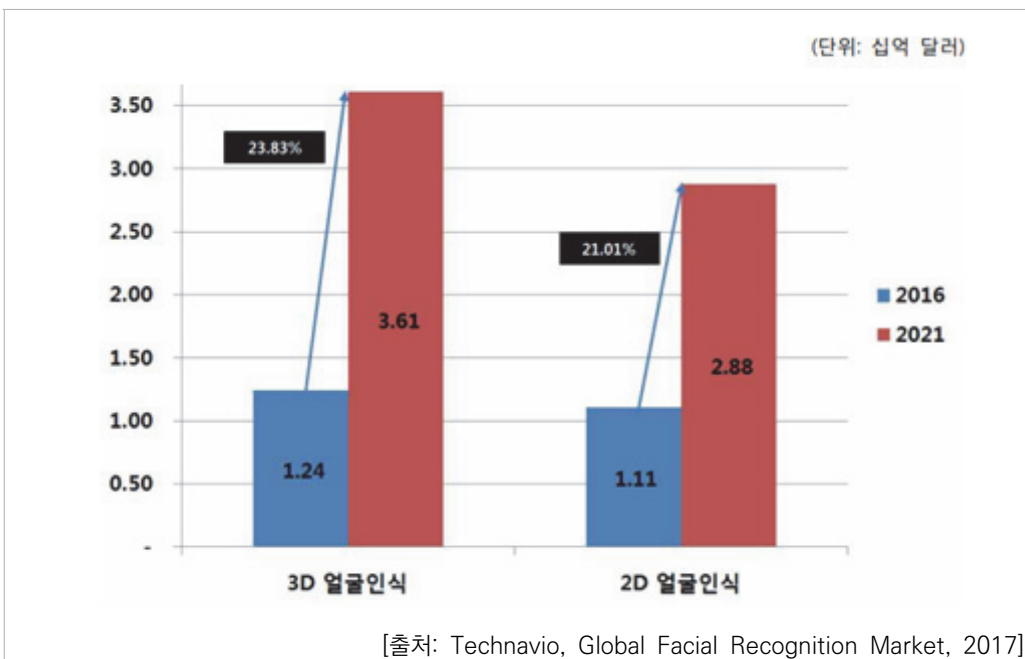
- 중국 농업은행은 얼굴인식 기능을 갖춘 ATM기기를 보급하여 일부 지점에서 카드발급, 환전, 펀드 환매 등의 업무를 얼굴인식으로 처리
- 알리페이, 마스터카드는 얼굴인식 기반의 결제서비스 제공

IT 분야 전문 시장조사기관 Technavio에 따르면 전 세계 얼굴인식 시장은 2016년 23억 5,000만 달러로, 세계 바이오인식 시장 규모인 127억 1300만 달러의 약 20%를 차지하고 있으며, 향후 연평균 성장률 22.53%로 증가하여, 2021년에는 64억 9,000만 달러로 성장할 것으로 전망하고 있다.

특히, 전 세계 얼굴인식 시장을 기술별로 살펴보면, 2차원 얼굴인식과 3차원 얼굴인식으로 구분되며, 2016년을 기준으로 3차원 얼굴인식이 52.78%로 가장 높은 점유율을 나타내고 있습니다. 3차원 얼굴인식은 2016년 12억 4,000만 달러에서 연평균 성장률 23.83%로 증가하여, 2021년에는 36억 1,000만 달러로 확대될 것으로 전망되고, 2차원 얼굴인식은 2016년 11억 1,000만 달러에서 연평균 성장률 21.01%로 증가하여, 2021년에는 28억 8,000만 달러에 이를 것으로 전망하고 있다.

[그림] 글로벌 얼굴인식 시장의 종류별 시장 규모 및 전망

(단위: 십억 달러)



[표] 글로벌 얼굴인식 응용 분야별 시장 전망

(단위: 백만달러)

분야	2015년	2016년	2017년	2018년	2019년	2020년	CAGR(%)
정부	334.7	383.5	432.3	477.3	522.4	566.7	11.1
출입국심사	419.6	480.6	541.5	597.7	654	709.3	11.1
군사/국방	188.9	225.2	261.5	300.1	338.6	380.1	15
건강관리	171.3	205.6	239.9	277.0	314.1	354.6	15.7
금융/회계	123.1	150.3	177.5	208.7	239.9	275.3	17.5
소비자가전	166.7	195.9	225.1	254.6	284.1	314.8	13.6
보안(가정용)	46.4	55.4	64.3	73.9	83.5	93.9	15.1
보안(상업용)	50.9	60.6	70.3	80.6	90.9	102.1	14.9
기타	20	23.7	27.4	31.3	35.2	39.4	14.5
합계	1,521.6	1,780.7	2,039.8	2,301.3	2,562.7	2,836.2	13.3

[출처: Market And Markets, "Next Generation Biometrics Market - Global Forecast 2020", 활용 KISTI작성]

한국 과학기술정보연구원(KISTI)은 세계 얼굴인식 시장 규모 중 한국이 점유하고 있는 비율(2010년 4.5%-2015년 4.8%)을 고려하여 국내 얼굴인식 시장 규모를 분석한 결과 국내 얼굴인식 시장 규모는 2015년 868억 원에서 2020년 1,514억 원으로 증가하여 연평균 11.8%씩 성장할 것으로 전망하고 있다.

KISTI에 따르면 여러 분야 중 가장 성장하고 있는 세계 출입국시장에서의 얼굴인식 솔루션의 규모는 2019년 약 6백만 달러, 2020년 709.3백만 달러로 성장할 것으로 예상된다.

[표] 국내 얼굴인식 시장 전망

(단위: 백만원)

구분	2015년	2016년	2017년	2018년	2019년	2020년	CAGR(%)
국내 얼굴인식	86,873	100,116	113,432	126,000	138,707	151,417	11.8

[출처: Market And Markets, "Next Generation Biometrics Market - Global Forecast 2020", 활용 KISTI작성]

얼굴인식 등 바이오인식 산업은 통신 시스템 업체들이 전방산업인 무인발급기, 현금 인출기, 모바일 인증, AFIS 및 전자여권 솔루션, 출입국 관리에 서비스를 제공하기 위해 후방산업인 바이오인식, 센서, 스마트카드 임베디드, 홈네트워크, 텔레메틱스 등 유무선 정보통신망 산업 등의 업체와 연결되어 산업의 Supply Chain을 형성 중이며, 바이오인식 엔진을 기반으로 바이오정보를 이용한 통합 솔루션 개발 업체의 약진이 두드러지는 추세이다.

전 세계적으로 얼굴인식 시장은 향후 다양한 분야에서 지속적으로 성장할 전망이며, 특히 출입국 관리 등의 공공과 모바일에서의 사업화를 위한 활용처를 찾아 집중할 필요가 있다. 이러한 얼굴인식 기술의 대중화를 위해서는 얼굴인식 기술 활용에 대한 고객의 심리적 불안감을 해소하는 노력과 함께 단일 기술로의 기술이전 및 사업화가 아닌 다양한 기술의 융합과 교류가 필요하다.

향후 10년간 금융, 헬스케어, 정부 부문이 바이오인식 시장의 주요 산업으로 자리매김할 것이며, 그중 얼굴인식이 가장 큰 매출비중으로 성장할 것으로 예상된다.

참고문헌

Technavio, Global Facial Recognition Market, 2017

Market And Markets, “Next Generation Biometrics Market - Global Forecast 2020”, 활용 KISTI작성

백영현, 간편결제에 적용되는 바이오인식 기술 현황, TTA저널 165, 2016.5

연구성과실용화진흥원, 생체인식기술 및 시장동향, vol.39, 2016.2

2019 국내 정보보호산업 실태조사

인 쇄 : 2019 년 12 월

발 행 : 2019 년 12 월

발행인 : 이 민 수

발행처 : 한국정보보호산업협회

서울시 송파구 중대로 135 IT벤처타워 9층

Tel: (02) 2142-0900

인쇄처 : 타라그래픽스

Tel: (02) 6268-1002

〈비매품〉

본 보고서의 내용은 사전 허가 없이 무단 전재 및 복사를 금합니다.

