

## 정보보호 산업 해외 거점 인프라 생성 연구

조창덕 · 박대우\*

### Building an Overseas Infrastructure Offices of the Information Security Industry

Chang-Duk Cho · Dea-Woo Park\*

Department of Converging Technology, Hoseo Graduate School of Venture, Seoul 06711, South Korea

#### 요 약

정보보호 산업은 기술집약적, 고부가 가치 산업이다. 한국은 우수한 ICT 기술과 다양한 사이버공격에 대응 경험과 기술을 보유하고 있어, 전 세계의 벤치마킹 대상이 되고 있다. 하지만 국내 정보보호기업의 영세성과 함께 지원인프라는 부족하다. 국내 정보보호 산업을 활성화하는데 일차적인 조건은, 해외진출이다. 부가가치가 높은 제품과 서비스의 해외 수출을 위해서는, 국내 IT 정보보호 산업의 해외진출 거점 인프라의 설립 추진이 필요하다. 국내 정보보호 산업을 분석해보니, 자본의 영세성과 해외 현지 진출의 관료개혁, 관련 정보, 인력 부족이 문제점으로 나타났다. 무료 AS기간의 비용까지 합치면, 사실상 손실이 발생한다. 따라서 정보보호 산업 해외 거점의 인프라 구축에 관한 연구가 필요하다. 해외 거점의 인프라의 선정 방법과 선정 원인을 분석한다. 해외 거점의 인프라를 활용하여 부가가치를 올릴 수 있고, 정보보호 산업 중소기업들이 수출을 활성화하기 위한 해외 거점의 인프라를 연구를 한다.

#### ABSTRACT

The information security industry is technology-intensive, high value-added industries. South Korea's response has excellent ICT skills and experience and skills in a variety of cyber attacks, has become a benchmark in the world. However, the small size of the domestic information security company, supporting infrastructure is lacking. Domestic information security industry is the primary condition to activate the export. For the export of high value-added enterprise information security products and services, it is necessary the establishment of the domestic IT information security infrastructure of the industrial promotion is based overseas. Come to analyze the domestic information security industry, capital of this small, market reclamation of overseas expansion, information, manpower shortage was a problem. This fact, combined losses caused by cost-free period AS. Therefore, the study on information security in the infrastructure industry overseas bases is necessary. How to select and analyze the causes of infrastructure in selected overseas offices. By utilizing the infrastructure of overseas bases, can raise the added value of the products and services of the Information Security company, we can enable the export of small and medium Information Security company from overseas offices.

**키워드** : ICT, 정보보호 산업, 해외 거점, 인프라

**Key word** : ICT, information security industry, overseas offices, infrastructure

접수일자 : 2015. 11. 30 심사완료일자 : 2015. 12. 21 게재확정일자 : 2016. 01. 04

\* **Corresponding Author** Dea-Woo, Park(E-mail:prof\_pdw@naver.com, Tel:+82-2-2059-2352)

Department of Converging Technology, Hoseo Graduate School of Venture, Seoul 06724, South Korea

**Open Access** <http://dx.doi.org/10.6109/jkiice.2016.20.1.103>

print ISSN: 2234-4772 online ISSN: 2288-4165

©This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License(<http://creativecommons.org/licenses/by-nc/3.0/>) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.  
Copyright © The Korea Institute of Information and Communication Engineering.

## I. 서론

대한민국은 정보통신기술(ICT: Information and Communication Technology)의 발전으로 인해 UN의 전문기구인 국제전기통신연합(ITU: International Telecommunication Union)이 조사한 정보통신기회지수( ICT Opportunity Index) 발표에서 2011년부터 2013년까지 전 세계 160 국가 중 1위를 차지하였다. 160 국가의 ICT에 대한 접근성, 이용도, 역량 부문 측면에서 제일 우수한 성적을 받았다[1].

그러나 ICT 기술발전에 따른 부작용을 동반되었다. 한국은 3.4DDoS(Distributed Denial of Service) 공격, 7.7DDoS 공격, 카드 3사의 1억2천 만건 개인정보유출 사건, 2014년 말에 한국수력원자력의 국가기밀정보유출 사고에서 보는 바와 같이, 메모리 해킹 공격(Hacking Attack)[2]과 APT(Advanced Persistent Threat)공격[3]이 발생하였고, 피싱, 파밍, 스미싱 공격[4]과 같은 사이버 사기[5], 스마트폰에서 정보탈취 및 스미싱 공격[6], 개인정보 유출 공격[7]과 같은 지식정보사회의 역기능[8]이 발생하고 있어, 정보보호 산업의 육성은 더욱 필요하다.

정보보호 산업은 기술집약적, 고부가 가치 산업으로 국내 ICT 산업 및 국가 경쟁력을 향상시키는 주력 산업으로 각광받고 있다. 대한민국은 우수한 ICT 기술을 보유하고 있고, 다양한 사이버공격에 대응 경험을 가지고 있어, 세계로부터 벤치마킹 대상이 되고 있다[8].

하지만 국내 정보보호기업은 자본금의 영세성과 지원 인력의 부족, 자금 등 지원인프라는 부족하다.

이러한 국내 정보보호 산업을 활성화하는데 필요한 일차적인 조건은 해외진출이다.

부가가치가 높은 해외진출을 위해서는, 국내 IT 정보보호 산업의 해외진출 거점 인프라의 설립 추진이 필요하다. 국내 IT 정보보호 산업의 자본의 영세성과 해외 현지 진출의 판로개척, 관련 정보, 인력 부족의 문제점으로 나타났다. 무료 AS기간의 비용까지 합치면, 사실상 손실이 발생한다.

따라서 정보보호 산업 해외 거점의 인프라 구축에 관한 연구가 필요하다. 해외 거점의 인프라의 선정 방법과 선정원인을 분석한다. 해외 거점의 인프라를 활용하여 부가가치를 올릴 수 있고, 정보보호 산업 중소기업들이 수출을 활성화하기 위한 연구를 한다.

## II. 국내외 정보보호시장 분석

### 2.1. 국내 정보보호기업과 시장

정보보호 관련 기업체의 자본금 규모를 조사한 결과 표 1과 같이 자본금 10억 미만 기업이 461개(70.6%), 10억 이상 50억 미만 기업이 142개(21.7%), 50억 이상 100억 미만 기업이 21개(3.2%), 100억 이상 기업이 29개(4.4%)인 것으로 조사되었다. 자본금이 50억 미만인 기업은 정보보안 92.2%, 물리보안 92.4%로 대부분을 차지함을 알 수 있다[9].

**Table. 1** Size of information security company capital Status (Unit : number %)

division	Information Security		Physical security	
	Company number	ratio(%)	Company number	ratio(%)
Less than 1 billion	185	72.3	276	69.5
Less than 1 billion to 5 billion	51	19.9	91	22.9
Less than 5 billion to 10 billion	8	3.1	13	3.3
More than 10 billion	12	4.7	17	4.3
total	256	100.0	397	100.0

2014년 국내 정보보호시장은 약 7.6조원(물리보안 5.9조, 정보보안 1.7조)이다. 국내 정보보호시장 성장률은 3년 평균 15%에서 7.1%로 감소되었고, 수출증가율도 8%에서 1.7%로 감소 중에 있다. 정보보안 기업의 경우 249개(97.3%)가 법인사업체, 7개(2.7%)가 개인사업체였으며, 물리보안 기업의 경우 340개(85.6%)가 법인사업체 57개(14.4%)가 개인사업체인 것으로 조사되었다[8]. 또한 국내 정보보호 기업의 지역별 분포를 조사한 결과 서울과 경기도 기업이 많은 것을 알 수 있다.

### 2.2 세계 정보보호시장과 국내 정보보호기업 수출

세계 정보보안 시장 규모는 2017년까지 연평균 8.5% 성장해서 932억달러에 달할 것으로 전망되며, 미국은 2013년 현재 전 세계 약 42%를 차지하고 있는 최대 시장이다.

세계 정보보호 시장규모는 2013년 668억달러로 2017년까지 연평균 8.5% 성장할 것으로 전망된다. 정보보호 시장을 574억달러 규모로 추산했으며 2017년까지 연평균 8.5% 성장해 932억달러에 달할 것으로 전망[9]했다.

정보보호 산업 수출액은 2013년 1,494,456백만 원에서 2014년에는 1.7% 증가한 1,520,245백만 원이 될 것으로 예상된다. 이 중에서 정보보안 수출액은 2013년 70,422백만 원에서 2014년 76,574백만 원으로 8.7% 증가하였으며, 물리보안 매출액은 2013년 1,424,034백만 원에서 2014년 1,443,671백만 원으로 1.4% 증가하였다. 2014년 전체 수출액에서 물리보안 수출액은 95% 이상으로 정보보안 수출액보다 매우 큰 것으로 나타났다.

정보보안의 경우 권역별 수출비중의 52% 가량이 일본에 편중되어 있으며, 물리보안의 경우 권역별 수출비중의 46% 이상은 유럽, 미국으로 편중[9]되어 있는 것으로 나타났다.

정보보호 산업 수출액은 2011년 1,190,000백만 원에서 연평균 9.0%씩 성장하는 등 지속적으로 성장하고 있다. 이 중에서 정보보안 매출액은 2011년 45,000백만 원에서 연평균 19%씩 성장하고 있으며, 물리보안 매출액은 2011년 1,145,000백만 원에서 연평균 8%씩 성장하고 있으나, 2011년에서 2012년으로 급격히 증가하다가 2012년부터 증가폭이 낮아지고 있는 것은 엔화 약세 및 중국 제품의 저가 공세 등이 원인으로 분석[9]되고 있다.

**Table. 2** Information Security Industry Exports by Country (Unit: KRW million,%)

division	Information Security				Physical security			
	2013년		2014년		2013년		2014년	
Japan	49,181	70.4	39,819	52.0	164,154	11.1	228,100	15.8
China	4,890	7.0	8,576	11.2	136,056	9.2	167,466	11.6
USA	3,563	5.1	6,356	8.3	412,603	27.9	412,890	28.6
Europe	1,607	2.3	3,522	4.6	365,280	24.7	245,424	17.0
etc.	10,619	15.2	18,301	23.9	400,772	27.0	389,791	27.1

표 2의 정보보안과 물리보안 수출 현황에서 미국의 수출이 28.6%로 가장 높고, 다른 지역은 고른 분포를 보이고 있다. 물리보안 분야별로 DVR 제품이 수출 시장에서 차지하는 규모가 2013년 31.8%인 452,508

백만원으로 가장 크며, 그 다음으로는 카메라 제품이 22.0%인 312,696백만원[9]으로 나타났다.

수출 증가율에서는 알람/모니터링 제품과 기타 제품, 주변장비 제품이 가장 큰 증가율을 기록하고 있다. 정보보호 관련 기업의 설립 근거별 현황을 조사한 결과 589개(90.2%)가 법인사업체, 64개(9.8%)가 개인사업체인 것으로 조사[10]되었다.

**2.3. 국내 정보보호 기업의 해외 진출 필요성**

정보보호 산업의 시장 규모 측면에서 인프라 보호가, 성장을 측면에서는 인증·접속 관리 및 네트워크 서비스 장비 분야가 활발한 성장 예측된다. 세계 사이버보안 시장 성장에 따라 해외 시장에 진출하여 국내 정보보호 산업을 육성하여야 하는 것이다.

**Table. 3** World Information Security Industry sectoral market trends (unit : millions of dollars)

	2015	2016	2017	2018
Authentication access management	3,331 (4.3%)	3,596 (4.3%)	3,883 (4.3%)	4,159 (4.3%)
Infrastructure Protection	14,352 (18.6%)	15,259 (18.3%)	16,145 (18.0%)	17,101 (17.6%)
Network Security	9,714 (12.6%)	10,304 (12.4%)	10,923 (12.2%)	11,524 (11.9%)
Security Services	43,933 (57.1%)	48,071 (57.8%)	52,682 (58.6%)	57,884 (59.6%)
Consumer Security SW	5,654 (7.3%)	5,945 (7.1%)	6,217 (6.9%)	6,479 (6.7%)
The entire information protection	76,984 (100%)	83,175 (100%)	89,850 (100%)	97,147 (100%)

표 3과 같이 세계 정보보호 산업 분야별 시장 동향 분석에서 사이버보안 산업은 미국 주도의 산업으로 전체 시장의 44%를 차지하고 있으나 북미와 서유럽 위주 시장에서 사이버보안 산업의 성장이 가속화 되고 있다.

한국의 정보보호 산업과 기술력은 미국, 유럽(EU) 등 선진국 대비해서 기술격차는 있으나, 빠르게 성장하는 신규 ICBM 사회로의 발전이 되면서, ICBM 이용자를 위한 신종 해킹 대응기술 개발이 필요하며, 지능화·고도화되는 사이버 공격에 대한 사전 역량을 강화하고, 침해사고 발생 시 신속한 탐지 및 복구를 위한 정보 패러다임의 변화로 정보보호 산업의 해외진출 방안 [1]이 필요한 시점이다.

해외 국가별 정보보호 제품의 수출 현황을 조사한 결과 정보보안 기업은 일본에 수출하는 기업 수가 전체 수출 기업의 52.0%를 차지하는 것으로 나타났다. 물리 보안 기업은 유럽과 미국 시장에 수출 비중이 높은 것으로 조사되었다.

#### 2.4. 국내 정보보호 기업의 해외 진출 애로사항

2014년 11월 발생한 소니 픽처스 해킹 사건은 GOP라 지칭하는 해킹그룹에 의해 내부 전산망 마미 및 미 개봉 영화 3편이 유출되는 등 최소 2,200억원(NYT보도)의 피해가 발생한 것으로 산정하였다.

세계 각국은 국가사이버보안 전략을 수립하여 이행하고 있으며, 정보보호 산업도 높은 성장세를 보일 것으로 전망된다. 글로벌 사이버보안 시장 규모는 290조원(물리/융합보안 212조원, 정보보안 78조원)이며, 연평균 8%의 성장세를 기록 (Gartner, Forecast Information Security)할 것으로 예측한다.

국내 정보보호 기업의 해외 진출 애로사항을 5점 만점으로 점수수준으로 조사를 하였으며 표 4와 같이 결과가 나왔다. 해외 진출의 판로개척이 4.48로 제일 높았으며, 인력 부족이 4.25, 해외진출을 위한 관련정보, 국제표준 및 인증획득이 4.10, 현지 법 및 제도 이해부족이 4.07을 기록[9]하고 있다.

**Table. 4** IT information security industry abroad difficulties Scores

Bottleneck problem	Scores level
According to a falling exchange rate profitability	3.13
Liquidity funds shortage	3.50
Burden of tariff Customs formalities	3.77
Lack of intellectual property rights protection capacity	3.83
The world economic instability, and a slowdown	3.91
Local laws and institutions	4.07
Acquiring international standards and certification	4.10
Relevant information for overseas expansion	4.25
Manpower shortage	4.39
Market reclamation	4.48

물리·융합 보안 산업은 ICT 응용기술 개발능력이 뛰어난 우리나라 기업에 가장 적합한 분야이다. 하지만 국내 시장규모가 세계시장의 1.9% 수준에 불과하고, 국내 중소기업으로 구성되어 있어, 정부의 정책적 지원, 전문 인력 양성 및 원천기술 연구개발에 대한 지원이 지속적으로 필요한 실정이다.

### III. 해외진출 권역별 거점 인프라 추진

#### 3.1. 해외 권역별 국가 거점 인프라 추진 필요성

대한민국 대통령의 중동(2015년), 중남미(2015년) 등 해외 순방을 계기로 발굴된 협력수요 및 한국형 정보보호 기업의 현지진출 지원이 필요하다. 또한 정보보호기업 해외진출 간담회시, 해외진출에 실질적으로 필요한 현지 업무를 지원할 전문가 파견 필요성 제기되고 있다.

표 5는 해외 권역별 국가 거점 인프라 추진 필요성을 정리 한 내용이다. 정보보호 분야의 특수성인 해외 진출 시 기술과 해외 시장, 국가 간 협력 필요 사항을 고려 시, 전문가 파견을 통한 전담지원의 필요성이 있다.

#### 3.2. 해외 권역별 국가 거점 인프라 주요 업무 분석

정보보호 기업의 해외거점 주요 거점 인프라 업무 내용을 분석해 보면 다음과 같다.

- 해당국가 및 인근국가의 정부발주 정보보호 프로젝트 수주 지원한다.
- 현지인력 정보보호 산업 현지진출지원 역량 강화(정보보호관련 교육 등)한다.
- 정보보호 해외진출을 위한 정부 간 협력(MoU, 협력사업 발굴)한다.
- 정보보호업체 현지 지사 역할(현지 바이어 발굴, 진출업체 현지 활동 대행)을 한다.
- 현지 정보보호 관련 정보 조사(현지 시장동향, 법제 인증 등 제도관련 정보)한다.
- 주요 국제기구 (OECD, IDB 등)에 정보보호 전문인력 파견 및 공조활동(컨설팅, 초청연수 등 역량개발사업)을 통해, 우리기업의 해외진출 기회 발굴한다.
- 진출 전략국가 중심으로 구축될 해외거점과 연계, 국제기구와의 협력사업 발굴 및 국내 기업의 참여 기회를 확대한다.

**Table. 5** Overseas countries based infrastructure promoting regional needs

Region	Based Infrastructure, promote the need	country
Mid east	<ul style="list-style-type: none"> <li>Plants, Construction sector, including government-led information security solutions and products entering the promotion business</li> <li>(UAE) VIP tour of follow-up projects to the Middle East's largest market</li> <li>(Oman) Joint Promotion nearby countries entering the market as a base to advance information security experience</li> <li>(Saudi Arabia, Qatar) Information protection is a high demand for Korea industry cooperation, funding leverage various information security projects promoted</li> </ul>	Qatar, Saudi Arabia, Kuwait, etc.
Africa	<ul style="list-style-type: none"> <li>Already entered the country (Rwanda), the Best Practice neighboring countries Tuesday to promote expansion and ODA projects associated support (up to regional demand)</li> <li>(Rwanda, Tanzania), Korea is a high demand for cooperation and joint expansion possibilities in the African market has already entered the country</li> <li>(EAC countries, Ethiopia) entering high potential to leverage the Rwanda case, various projects promoted by MDB funds</li> </ul>	EAC region: (Tanzania, Uganda, Kenya, Burundi) Ethiopia, etc
Central America	<ul style="list-style-type: none"> <li>Recently, Broadband networks, such as areas where ICT Infra is expanding rapidly, the expected high demand for security-related information (Latin American Ministers Meeting utilization)</li> <li>(Nicaragua), Information protection Project currently underway (F / S plans, etc.), it is easy to enter neighboring countries over the next base advantage</li> <li>(Costa Rica, Colombia) PKI, information security master plan, leveraging consulting, advisory, such as facilitating overseas opportunities</li> </ul>	Costa Rica, Colombia, Venezuela, Dominica, etc
South America	<ul style="list-style-type: none"> <li>Since higher VIP tour, the demand for cooperation, information security expert workshops and consulting needs through the market opportunities</li> <li>(Peru), and signed MOU and the increasing demand on cooperation and exchanges, promote Best Practice Tue required expansion in Latin America</li> <li>(Chile) Business environment and market environment is easy, Information protection needs require intensive support during excavation area of the company (leverage foothold in South America)</li> </ul>	Brazil, Chile, Argentina, etc
South east Asia	<ul style="list-style-type: none"> <li>Support-related information that has already been done (consulting, training, F / S, etc.) utilized, can promote industrialization, expansion SI joint enterprises and markets available</li> <li>(Vietnam) ensuring Information protection related inter-governmental cooperation, Korea Information protection ICT and high demand</li> <li>(Cambodia, Myanmar) demands new projects already conducted excavations easy to take advantage of the various consulting and advisory activity results</li> </ul>	Cambodia, Myanmar, etc.
Southwest Asia	<ul style="list-style-type: none"> <li>Information security part cooperation, and project Employer recent increase and advance the short term, expect a substantial area</li> <li>(Singapore) to the Southeast Asian market center, the existing infrastructure (NIPA center) and labor utilization are possible and easy to neighboring jurisdictions</li> <li>(Brunei) information security-related projects are expected orders, information security-related international activities is being actively promote the cooperation destination country.</li> </ul>	Brunei, Malaysia, Indonesia, Bangladesh, etc.
Europe	<ul style="list-style-type: none"> <li>Often information security developed countries, technical exchanges, M&amp;A Overseas Empowerment is available through the local information security companies</li> <li>(Eastern Europe)Romania, Estonia, etc. S/W and Information security powerhouse excavation technology exchange and cooperation necessary</li> <li>(UK, Germany, France)The European ICT field powerhouse in Information security cooperation and ongoing information sharing needs Trend</li> </ul>	European Areas
Developed-markets	<ul style="list-style-type: none"> <li>Technology, distribution channels are considered an important market characteristics, customer base formation, a professional exhibition support enhanced</li> <li>(USA) IR, incubating, with a focus on technology exchanges Information protection advance support local businesses and existing infrastructure (NIPA center) utilization</li> <li>(Japan) countries with top Information protection companies exporting high demand</li> </ul>	USA, Japan

### 3.3. 정보보호 전략 국가의 거점 인프라 추진

대한민국 정부에서 지정한 권역별 국가협력전략 대상 국가는 해외 시장 개척인 KOTRA, 중소기업청, 미래 창조과학부, KISA, 산업자원부 등의 해외 IT지원센터(NIPA) 등의 인프라를 활용하여야 한다.

대한민국의 대외 정책은 경제, 외교, 문화, 정치적인 이해관계 등을 고려하여, 해외 각국에 대한 대외 정책의 우선순위를 설정하고 있으며, 경제적 차원의 실리 외교와 지원 정책을 정하고 있다. 한-중 FTA 타결로 한국의 FTA 체결국이 52개국으로 확대된 만큼 기업의 FTA 활용을 위한 KOTRA의 지원이 확대되고 있다.

이에 따라서 한국국제협력단(KOICA), 수출입은행에서는 이러한 순위를 반영하여 각종 자금 원조 및 차관 지원을 하고 있다.

정보보호 기업의 해외 진출 전략도, 권역별 국가의 정책적 우선순위를 반영하면, 정부의 중장기 지원 정책과 예산 지원의 혜택을 받을 수 있고, 이를 통하여 정보보호 기업의 해외 진출 전략진출의 효과를 높이기 위해, 기존 KOTRA의 해외진출 거점 인프라와 함께, 해외진출 권역별 거점 인프라의 설립 방안을 도출할 수 있다.

KOTRA의 10대 권역은 중국, 미국, 일본, 유럽, 중남미, 독립국가연합(CIS), 동남아, 서남아, 중동, 아프리카이며, 해당 지역의 성장가능성과 위협요인 별로 정보보호 기업의 해외진출 전략을 발굴해야 한다.

특히, 정보보호 기술력이 앞서고, 정보보호 세계시장을 선점하고 있는 선진국과의 경쟁을 피하고, 정보보호 제품의 틈새시장에 중점을 둔다면, 권역별 국가협력전략(CPS) 대상 국가의 해외진출 권역별 거점 인프라의 지부를 설치하는 것도 방안이다.

## IV. 해외진출 권역별 거점 인프라 추진

정보보호 산업 해외진출을 위한 권역별 진출 거점 인프라 주요 후보 전략국가를 중심으로 정보보호 해외진출 거점을 마련한다.

표 6에 분류한 바와 같이 거점 국가의 인프라 후보 지역으로는 중동(UAE), 중남미(코스타리카), 아프리카(탄자니아), 동남아(베트남, 우즈베키스탄) 등을 거론할 수 있으며, 정보보호 산업의 기술과 제품 및 서비스

에 대한 프로젝트 수주활동 중인 국가에 우선적으로 구축하고, 추후 선진시장(미국, EU, 일본), 아프리카(르완다), 중남미(페루), 중동(오만), 동남아(싱가포르) 등을 확대 후보로 한다.

**Table. 6** Country cooperation strategy target countries and regional information security strategy, national enterprises

Region	Regional country cooperation strategy (CPS) target countries	Information security Strategy Country
Asia (Southeast Asia, Central Asia) (9)	Nepal, East Timor, Laos, Mongolia, Bangladesh, Vietnam, Bhutan, Solomon Islands, Sri Lanka, Indonesia, Cambodia, Pakistan, the Philippines, Malaysia, Azerbaijan, Uzbekistan	China, Vietnam, Mongolia, Bangladesh, Thailand, Malaysia, Myanmar, Indonesia, Uzbekistan
Mid east (4)	Saudi Arabia, UAE, Qatar, Kuwait, Iraq	Saudi Arabia, UAE, Qatar, Kuwait
Latin American(4)	Bolivia, Ecuador, Colombia, Paraguay, Peru	Peru, Nicaragua, Chile, Brazil
Africa (3)	Ghana, Nigeria, Congo, Rwanda, Mozambique, Ethiopia, Uganda, Cameroon	Uganda, Tanzania, Ethiopia
Developed-markets (3)	United States, Japan, Europe(EU)	United States, Japan, Europe(EU)

## V. 결론

국내 정보보호 산업을 활성화하는데 일차적인 조건은 해외진출이다. 해외진출이 필요한 이유는 국내 IT 정보보호 산업의 자본의 영세성과 해외 현지 진출의 판로개척, 관련 정보, 인력 부족 등의 문제점으로 나타났다. 따라서 정보보호 산업 해외 거점의 인프라 설정을 위한 선정 방법과 선정 원인을 분석하였다.

본 연구는 해외 거점의 인프라를 활용하여 부가가치를 올릴 수 있고, 정보보호 산업 중소기업들이 수출을 활성화하기 위한 해외진출 권역별 거점 인프라 추진을 연구하였다.

REFERENCES

- [ 1 ] Dea-Woo, Park, Interim Report\_2015 Broadcasting Communication Policy Research, Information Security Industry Overseas Study Support, Sep. 2015.
- [ 2 ] Korea Internet & Security Agency, "Monthly analysis and trend of Internet incidents : March, May, June", Korea Internet & Security Agency, Korea, March, May, June 2013.
- [ 3 ] Dea-Woo, Park, Sung-Young Yang, "Hacking Aattack Trends Analysis of Mobile Smishing and Security Measures," in *Proceeding of the Conference on Information and Communication Engineering*, Busan: South Korea, pp. 154, Oct. 2015.
- [ 4 ] Dea-Woo, Park, Analysis on Mobile Forensic of Smishing Hacking Attack, *Journal of the Korean Institute of Information and Communication Engineering*, vol., 8, no. 12, pp. 2878-2883, Dec. 2014.
- [ 5 ] Korean National Police Agency Cyber Bureau, "Coping with smishing", [Internet]. Available: <http://www.netan.go.kr/>, the National Police Agency, July, 2015.
- [ 6 ] In-Woo Park, Dea-Woo Park, "A Study of Intrusion Security Research and Smishing Hacking Attack on a Smartphone", *Journal of the Korea Institute of Information and Communication Engineering*, vol., 17, no. 2, pp. 399-406, Mar, 2013.
- [ 7 ] Dea-woo Park, "Guideline for Countermeasures against Smishing Incident", CJK IT Standards Meeting, South Korea, April, 2014.
- [ 8 ] Dea-Woo, Park, Information Security industry overseas support and necessity standardization, National Cyber Security Policy Forum Workshop, November, 2015.
- [ 9 ] Privacy foundation, 2015 National Information Security White Paper, Size of information security company capital Status, KISIA, April, 2015.
- [ 10 ] Privacy foundation, 2015 National Information Security White Paper, Information Security Industry Sales Result, KISIA, April, 2015.



**조창덕(Chang-Duk Cho)**

1999년 : 신안산대학교 겸임교수, 4년  
 2009년 : 애경레지콘(주)대표이사 역임  
 2010년 : IT업체(베라카) 전무이사 역임  
 2013년 ~ 현재 : 티아이(주) 대표  
 2013년 ~ 현재 : 호서대학교 벤처대학원 박사과정  
 ※ 관심분야 : 정보보호, 이동통신보안, IT응용환경, IT융합, 융합보안, 시스템통합, 시스템 유지보수



**박대우(Dea-Woo Park)**

2004년 : 송실대학교 컴퓨터학과(공학박사)  
 2004년 : 송실대학교 겸임교수  
 2006년 : 정보보호진흥원(KISA) 선임연구원  
 2007년 ~ 현재 : 호서대학교 벤처대학원 교수  
 ※ 관심분야 : Hacking, Forensic, CERT/CC, 침해사고대응, e-Discovery, 국가사이버안보, Cybersecurity, 정보보호, 이동통신보안, 융합보안, IT융합