

 미래창조과학부 http://www.msip.go.kr		<h1>보도자료</h1>		 대한민국 재도약의 힘, 창조경제	
보도일시	2016. 6. 9.(목) 11:00부터 보도해 주시기 바랍니다.				
배포일시	2016. 6. 7.(화)	담당부서	정보보호기획과		
담당과장	허성욱 (02-2110-2910)	담당자	임재덕 사무관(02-2110-2911)		

정보보호 산업정책, ‘창업과 해외진출’ 에 집중 - 미래부, 향후 5년간 추진할 “K-ICT 시큐리티 2020” 발표 -

- ◇ 정보보호 산업정책, ▲ 창업활성화를 통한 글로벌 경쟁력 강화
▲ 정보보호 투자 확대 및 신시장 창출 ▲ 내수 위주에서 글로벌 진출로 시장 확대 등에 주력
- ◇ 이를 위해 향후 5년간 추진할 10대 정책과제 선정·발표
 - ① 글로벌 창업 프로그램과 연계하여 20년까지 스타트업 100개 육성
 - ② 국제 공동연구를 통한 지능형·융합형 핵심 보안기술 개발
 - ③ 정보보호 예산 확대 및 보안성 지속서비스 대가 현실화
 - ④ 의료, 교통 등 5대 ICT 융합산업의 보안 강화
 - ⑤ 지능형 CCTV, 바이오인식 등 물리보안 및 차세대 인증산업 육성 지원
 - ⑥ 글로벌 기업과의 전략적 제휴 및 해외시장 진출 지원 확대
 - ⑦ ICT 강국 위상, 침해사고 대응 역량과 기업 주력 품목을 결합하여 “K-Security” 브랜드화 및 동반진출 추진
 - ⑧ 아프리카, 중남미, 중동, 동남아 등 해외진출 4대 전략 거점 구축 및 사이버보안 협력 네트워크(CAMP) 구성·운영
 - ⑨ 지능정보사회·융합보안 추세에 맞는 사이버 침해대응 역량 강화
 - ⑩ 범정부 협업 강화 및 법제도 개선

- 미래창조과학부(장관 최양희, 이하 ‘미래부’)는 6월 9일(목) 제8차 경제관계장관회의에서 향후 5년간 정보보호산업의 육성과 전문 일자리 창출을 견인할 「제1차 정보보호산업 진흥계획」(가칭 : K-ICT 시큐리티 2020)을 수립·발표하였다.
 - 이날 발표된 계획은 지난해 제정된 「정보보호산업의 진흥에 관한 법률」에 따라 수립된 법정계획으로, 기존의 정책들을 재점검·보완하여 2020년까지 추진할 기본계획이다.
- 최근 전세계적으로 사이버 위협은 양적 확대를 넘어 지능화, 은밀화되고 있으며, 사회적 혼란과 국가 안보를 위협하는 수준으로 발전하고 있다.
 - 이에 세계 주요 국가들은 정보보호 대응역량 강화와 함께 차세대 성장엔진으로서 정보보호산업을 정부 차원에서 적극 육성하고 있으며, 우리 정부도 그간 침해사고 대응 경험을 바탕으로 정보보호산업을 신성장 산업으로 육성하기 위해 “K-ICT 전략”의 핵심 산업으로 다양한 정책을 추진해왔다.
 - 그간의 노력에도 불구하고 정보보호산업은 ICT 산업에 비해 글로벌 경쟁력 확보가 더디게 진행되고, 성장률도 둔화되어 중장기 정책방향 재점검이 필요한 상황에 놓여있다.
- 이에 미래부는 범정부 차원에서 제1차 「정보보호산업 진흥계획」을 수립하고, 창업 활성화와 해외진출을 중심으로 정보보호산업의 경쟁력 강화와 일자리 창출을 적극 추진할 계획이다.
 - 「정보보호산업 진흥계획」의 주요 정책과제는 다음과 같다.

□ 첫째, **창업활성화 전략**으로서 침해대응 시설, 인력 양성기관 등을 집적한 **정보보호 클러스터** 조성을 추진하고, **글로벌 펀드 및 엑셀러레이터와 연계**하여 유망 **스타트업의 발굴에서 사업화까지** 전단계 지원을 강화할 계획이다.

○ 또한 스타트업, 중소기업의 핵심 기술과 인력 확보를 위해 **국제 공동연구와 범부처 공동 R&D**를 통해 지능형 보안 원천기술을 개발하여 **민간 이전을 확산**할 계획이며, 기존 대응 중심의 인력양성 체계에 **산업을 연계한 인력양성 전략**을 수립하였다.

□ 둘째, **정보보호 투자확대 및 신시장 창출** 전략으로서 공공부문의 **정보보호 예산을 지속 확대**하고, 민간의 **정보보호 투자에 인센티브** 지원을 확대할 계획이다. 유지보수비 외에 **보안성 지속서비스 대가**를 현실화하고 민·관 합동으로 **불공정 발주 관행 해소** 등 제값 주는 **문화 확산**을 추진할 계획이다.

○ 아울러 의료, 에너지, 교통, 홈·가전·제조 등 **5대 ICT 융합 제품·서비스** 개발시 **설계 단계부터 보안기능을 적용**하도록 추진하고, 지능형 CCTV, 바이오인식, 스마트카드, 빅데이터 기반 영상분석 등 **4대 미래유망 물리보안산업의 육성**을 지원할 계획이다.

□ 셋째, **그간 내수 중심의 시장 구조를 깨고 글로벌 진출로 시장 확대**를 추진한다. **글로벌 기업과의 전략적 제휴**를 추진하고, 한국의 강점인 **ICT 강국 위상 및 침해사고 대응 경험과 기업 주력품목을 결합한 “K-Security” 브랜드화**를 추진한다.

○ 아프리카, 중남미, 중동, 동남아 등 **4대 전략거점***을 중심으로 **디지털포렌식, 침해대응모델** 등 현지에 적합한 수출을 확대할 계획이다.

* 4개 거점 : 아프리카(탄자니아), 중동(오만), 동남아(인도네시아), 중남미(코스타리카)

○ 또한 수출 잠재력이 높은 개도국을 중심으로 **“사이버보안 협력**

네트워크” (CAMP*)를 구성·운영하여 **해외진출 플랫폼**으로 활용할 계획이다.

* Cybersecurity Alliance for Mutual Progress : 한국 주도의 글로벌 사이버보안분야 협력체로 신흥국 중심으로 '16년 7월 발족 예정('16년 25개국 → '20년 60개국)

□ 넷째, ICT 융합산업의 **지속적인 성장 생태계 조성**을 위해 **국가 사이버 침해대응 역량**을 강화한다. **지능정보기술을 활용**하여 **침해사고를 사전에 탐지·대응**할 수 있도록 대응체계 고도화를 추진한다.

○ 이와 함께, **공공 및 민간 기업간 사이버 위협정보 공유**를 확대하고, 이를 활용하여 기업이 제품을 개발할 수 있도록 지원할 계획이며, 국경을 초월한 사이버위협에 신속 대응하기 위해 **미·중·일 등 주요국의 사이버 대응기관과 국제 공조**를 강화할 계획이다.

○ 아울러, 정보보호의 중요성이 **소 산업으로 확대**됨에 따라 **범정부 차원의 협력**을 강화하고 **사이버위협정보 공유에 관한 법적 근거 마련** 등 새로운 ICT 환경을 반영한 **정보보호 법·제도개선**을 지속 추진할 계획이다.

□ 미래부는 이번 진흥계획을 통해 2020년까지 정보보호 창업기업 100개, **글로벌 중소기업 10개**를 육성하는 한편, 현재 1.6조원 규모인 **정보보호 수출규모를 4.5조원**으로 확대하고,

○ 스타트업 창업, 해외시장 진출 기업 확대, 정보보호 투자확대 등을 통해 **약 1만 9천개의 일자리** 창출할 수 있을 것으로 기대하고 있다.

□ **최양희 미래부 장관**은 “세계 최고의 사이버보안 강국으로 도약하기 위해서는 **튼튼한 ‘정보보호산업’이 반드시 뒷받침** 되어야 하며, 이번 전략 수립으로 우리나라 **정보보호의 패러다임을 혁신하는 전환점**이 마련되었다”라고 강조하면서,

○ “앞으로 미래부는 **정보보호산업을 창조경제의 새로운 블루오션**으로 집중 육성하여, **우리나라의 미래 먹거리 산업**으로 만드는데 최선을 다할 것”이라고 밝혔다.

붙임 제1차 정보보호산업 진흥계획(요약)

I 추진배경

- 미국, EU, 이스라엘 등 세계 주요국들은 정보보호산업을 차세대 성장엔진으로 인식하고 정부 차원에서 적극적인 투자를 추진 중
- 우리 정부도 그간 침해사고 대응 경험을 바탕으로 新성장 산업으로 육성하고자 'K-ICT 전략'의 핵심산업으로 다양한 정책을 추진
- 그러나 정부의 노력에도 불구하고 정보보호산업은 ICT 산업에 비해 글로벌 경쟁력 확보가 더디고, 국내산업 성장률도 둔화되어 기존 정책에 대한 평가·보완 및 중장기 정책방향 재점검 필요
- 또한 최근 지능정보사회의 도래, 융합산업의 발전에 따른 새로운 보안위협에 대응하기 위한 기술개발과 대응체계 마련이 시급

- ◆ 이에 「정보보호산업의 진흥에 관한 법률」에 따른 법정계획으로 제1차 「정보보호산업 진흥계획(’16~’20년)」을 수립하여,
 - 민·관 협력을 통한 산업체질 개선과 창업 활성화 및 해외진출 가속화로 정보보호산업의 경쟁력 강화와 양질의 일자리 창출 추진

II 현황 및 문제점

- 정보보호 투자 부족, 저가경쟁, 내수 중심 협소한 시장상황의 개선은 더디며, 최근의 매출 성장세도 둔화되는 추세
- 기업규모가 영세하며 공공 발주 중심 또는 규제 위주 시장 의존으로 글로벌 정보보호 기업으로 성장하지 못하는 한계
- 최정예 인력양성 체계를 확립하였으나, 산업 현장에 맞는 개발 인력은 여전히 부족하며 우수 인력은 창업을 기피하는 상황

◁ 정보보호산업의 개념 및 중요성 ▷

□ (개념) 사이버공간을 포함하여 우리 주변 실생활에서 정보를 보호하고 안전을 지키기 위한 기술 및 관련 제품을 개발·생산·유통하는 산업

○ (구분) ‘사이버보안’, ‘물리보안’, ‘융합보안’(사이버보안+他산업)으로 분류

					
네트워크·시스템 보안 관제·디지털 포렌식 등	영상감시, 바이오인식 무인전자경비 등	제조, 에너지, 교통, 의료, 홈·가전 등에 대한 보안			
사이버보안	물리보안	융합보안			

* 기존 해킹·바이러스 대응을 위한 사이버보안에서 물리보안과 융합보안으로 개념이 확장됨

○ (동향) 3차 산업이 ICT 기술과 연계·융합되면서 기존 사이버공간의 위험이 현실세계로 전이(轉移)되어 대부분의 제품에 보안이 필요

* 예) 홈·가전제품 해킹을 통한 개인정보 탈취, 스마트카 악성코드 감염으로 인한 오동작 유발 등

□ (중요성) 정보보호산업은 안전한 ICT 성장을 위한 ‘사이버보안’ 산업이자, 침해대응 경험을 적극 활용할 수 있는 유망한 미래 新성장동력

○ (사회안전산업) 수도, 철도, 지하철, 병원, 홍수관리 등 사회 기본 시스템의 안전을 담보하는 안전산업

※ 사이버 침해사고로 인한 경제적 피해규모는 연간 3.6조원(자연재해 피해액 1.7조원의 2배를 상회)

○ (사이버보안산업) 테러, 범죄, 재난, 해킹, 산업 스파이 등 非군사적 안보위협을 방어하고 국가의 사이버자주권과 직결되는 보안산업

○ (미래성장산업) ICBM* 환경변화로 3차 산업분야에 보안기술 적용이 요구되어 정보보호가 핵심경쟁력이며, 신산업을 창출하는 미래성장산업

* ICBM : 사물인터넷(IoT), 클라우드(Cloud), 빅데이터(Big Data), 모바일(Mobile)

※ IoT로 창출되는 부가가치는 '20년까지 약 1조9천억 달러로 전망(가트너, '13년)

Ⅲ 비전 및 전략

비전 정보보호가 기본이 되는 사회, 신성장 산업으로 육성

목표



전략

- ✓ 혁신적 아이디어가 사업화 될 수 있는 창업 환경 조성
- ✓ 내수 중심의 악순환 구조를 깨고 글로벌 전체로 시장 확대
- ✓ 침해사고 대응경험을 산업 경쟁력 제고로 전환

추진 과제

정보보호산업
생태계 혁신

<p style="text-align: center; color: blue;">< 글로벌 경쟁력 강화 ></p> <ol style="list-style-type: none"> ① 글로벌 스타트업 창업 활성화 ② 차세대 핵심기술 및 산업형 보안인재 확보 	<p style="text-align: center; color: blue;">< 투자 확대 및 新시장 창출 ></p> <ol style="list-style-type: none"> ③ 투자 확대 및 산업체질 개선 ④ 융합보안 내재화를 위한 지원체계 구축 및 시장확대 ⑤ 4대 물리보안 및 차세대 전자인증산업 육성
<p style="text-align: center; color: blue;">< 해외진출 촉진 ></p> <ol style="list-style-type: none"> ⑥ 정보보호산업의 글로벌 스탠다드화 ⑦ 「K-Security」 브랜드화 ⑧ 전략적점 활용 신규시장 확대 	<p style="text-align: center; color: blue;">< 지속성장 생태계 조성 ></p> <ol style="list-style-type: none"> ⑨ 국가 사이버 침해대응 역량 강화 ⑩ 정보보호 협업 거버넌스 강화 및 법제도 개선

정보보호산업
생태계 혁신

Ⅳ 정보보호산업 경쟁력 강화를 위한 10대 정책과제

① 창업활성화를 통한 글로벌 경쟁력 강화

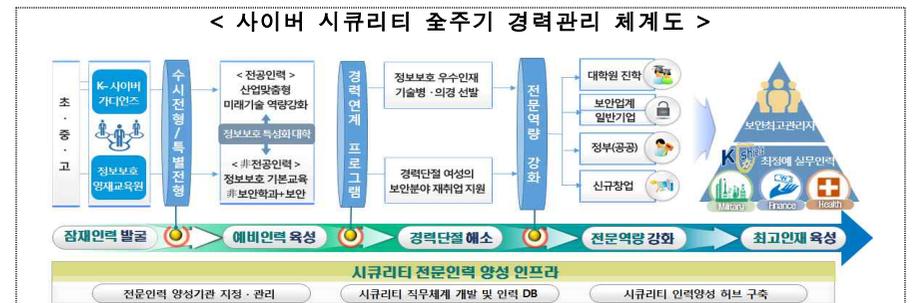
- (창업 활성화) 침해사고 대응시설, 인력 양성기관, 창업 지원센터 등을 집적한 정보보호 클러스터 조성으로 창업 지원 인프라 구축
- 글로벌 펀드, 해외 엑셀러레이터와 연계하여 유망 스타트업을 발굴하고, 처음부터 해외진출을 전제로 사업화 전단계별로 지원



- (차세대 기술 및 인재확보) 국제공동연구*, 범부처 공동 R&D 등으로 지능형·융합형 보안 원천기술을 확보하고 민간 이전 확산

* 지능형 사이버보안 대응기술(미국토안보부), IoT 보안기술(카네기멜론, UC버클리) 既추진중

- 생애 전주기 보안역량 성장체계를 구축하고 산업 연계형 교육 강화



② 정보보호 투자확대 및 신시장 창출

- (투자확대 및 체질개선) 공공부문의 정보보호 예산을 지속 확대하고, 민간의 정보보호 투자에 인센티브 확대 지원
 - 보안성 지속 서비스의 대가를 현실화하고 민·관 합동 모니터링으로 불공정 발주 관행 개선 등 제값 주는 문화 확산
- (융합보안 강화) 의료, 에너지, 교통, 홈·가전·제조 등 5대 ICT 융합 제품·서비스 개발시 설계 단계부터 보안기능을 적용하도록 추진
 - 융합보안 가이드라인 개발, 보안 시험·평가·인증 기준 마련

<융합보안 강화 방안>



- (물리보안산업 육성) 지능형 CCTV, 바이오인식, 스마트카드, 빅데이터 기반 영상분석 등 4대 미래유망 물리보안산업 집중육성
 - 핀테크, 사물인터넷(IoT) 등에 적용할 안전하고 편리한 차세대 전자인증 기술개발 및 사업화 지원

<물리보안 육성 방안>



③ 내수 위주에서 글로벌 진출로 시장 확대

- (정보보호산업의 글로벌화) 글로벌 기업과의 전략적 제휴 및 맞춤형 해외 시장 정보 제공을 확대하고, 글로벌 표준에 맞는 보안제품을 개발할 수 있도록 인증제도 개선
- (K-Security 브랜드화) 한국의 강점인 ICT 강국 위상, 침해사고 대응 경험과 기업 주력품목을 결합하여 “K-Security” 브랜드화 추진
 - 기업간 협업·제휴를 통해 제품을 패키지화하여 동반진출할 수 있도록 추진하고 공동마케팅 등 맞춤형 해외진출 지원 강화
 - 우수기업의 해외 인지도 확보 및 국제 전시회 개최, 유치 지원
- (전략거점 확보) 아프리카, 중남미, 중동, 동남아 등 4대 전략거점*을 중심으로 디지털포렌식, 침해대응모델 등 현지에 적합한 수출 확대
 - * 4개 거점 : 아프리카(탄자니아), 중동(오만), 동남아(인도네시아), 중남미(코스타리카)
- ODA 사업, 전자정부 수출, 플랜트 수출과 동반진출 지원
- 수출 잠재력이 높은 개도국을 포함한 “사이버보안 협력 네트워크”(CAMP)를 구성·운영하여 해외진출 플랫폼으로 활용
 - * Cybersecurity Alliance for Mutual Progress : 한국 주도의 글로벌 사이버보안분야 협력체로 신흥국 중심으로 '16년 7월 발족 예정('16년 25개국 → '20년 60개국)

< 권역별 중점 해외진출 사업 >



④ 지속성장 생태계 조성

- (국가 사이버 침해대응 역량 강화) 지능정보기술을 활용하여 사이버 침해사고를 사전에 탐지·대응할 수 있도록 대응체계 고도화
 - 사이버 위협정보 관련 공공 및 민간 기업간 공유를 확대하고, 이를 활용하여 제품을 개발할 수 있도록 지원
 - 국경을 초월한 사이버위협에 신속 대응하기 위해 미·중·일 등 주요국의 사이버 대응기관과 국제 공조 강화
- (범정부 협업) 정보보호의 중요성이 쏠 산업으로 확대됨에 따라 범정부 차원의 협력 강화 및 새로운 ICT 환경을 반영한 정보보호 법·제도개선 지속 추진

V 기대효과

- 정보보호 스타트업 육성, 핵심 원천기술 개발, 해외진출 지원 등을 통해 정보보호산업 글로벌 경쟁력 확보 및 시장 확대
 - 현재 1.6조원 규모인 정보보호 수출규모를 '20년까지 4.5조원으로 확대
- 정보보호 투자확대, 창업 활성화, 해외진출 가속화 등으로 2020년까지 약 1만9천개 이상의 일자리 창출 효과 기대
- 정보보호 기술, 인력, 대응 역량 강화로 안전한 산업 생태계 조성
- 지능정보기술을 활용한 정보보호 원천기술 확보를 통해 선진국과의 기술격차를 현 1.5년에서 0.2년으로 단축