정보보호 연구개발 이슈 및 추진방향

원유재, 이태진, 문기영
한국산업기술평가관리원

요 약

정부는 국내 정보보호 기술이 2018년 세계 시장 점유율을 3.2% 달성하는 목표를 정하고 이를 위한 기술개발 계획을 수립하였다. 이를 위하여 국내외 시장과 기술 경쟁력을 분석하여 세계일류 10대 제품을 선정하고 기술개발 로드맵을 정하였다. 본고에서는 10대 세계일류 제품과 이들의 개발 로드맵 그리고 2014년 추진 방향에 대해 알아본다.

Ⅰ. 서 론

사회기반 전반에 ICT의존도가 확산되면서 전세계적으로 사이버 공격에 의한 피해는 급증하고 있으며 사회안정과 국가 안위로까지 직결되고 있는 상황이다. 실제로 2011년 전세계적으로 발생한 사이버 공격은 55억 건으로 2010년 대비 81%나 증가하였고 온라인 금융사기나 아이디 도용과 같은 사이버 범죄로 인한 직간접적인 피해는 약 417조원으로 추정하고 있다. 국내의 경우도 2013년 발생한 3.20 사태로 인한 피해액은 많게는 8,051억 원까지 추정하고 있는 실정이다.

한편, 2012년 세계 정보보호 시장 규모는 유무선통신서비스 시장규모인 1,655억불을 초과하였는데, 성장률 측면에서 보면 국내는 지정학적 위험과 ICT 융합확산에 따른 높은 사이버위협 요인 등으로 세계시장 성장률인 10.5%를 상회한 14.6%에 다다를 전망이다. 그러나, 국내 정보보호산업의 현황은 세계 최고의 네트워크 인프라와 IT 강국 등의 긍정적인 요소에도 불구하고 수요측면에서 상대적으로 협소하고, 공급측면에서는 기술경쟁력 및 우수인력 확보가 지연되고 있으며, 구조적인 측면에서 영세한 산업구조의 악순환으로 인한 글로벌 경쟁력이 미흡한 상황이다.

따라서, 본 고에서는 정보보호산업 환경을 분석하고 기술개발 측면에서 환경을 극복하기 위한 방안을 도출하여 세계시장을 선도할 수 있는 목표를 정립하고, 목표를 달성하기 위한 기술개발 전략을 요약하여 기술하기로 한다.

Ⅱ. 환경분석

1. 정보보호의 개념과 범위

정보보호의 개념은 암호, 인증, 탐지, 인식, 감시 등의 보안기술이 적용된 제품을 생산하거나, 관련 보안기술을 활용하여 개인, 기업, 국가의 안전과 신뢰를 보장하는 서비스를 제공하는 기술을 말한다. 아울러, 정보보호의 범위는 네트워크, 시스템 보안 및 서비스와 이용자보호 등을 위한 정보보안, 안전, 안심생활을 지원하는 물리보안, 보안기술로 IT-융합 전통산업의 안전성과 신뢰성을 제공하는 융합보안을 포함한다.

2. 국내외 정보보호 시장환경

세계 정보보호 시장은 IDC에 의하면 2017년 2,851억불로 2012년 대비 약 1.6배 성장할 것으로 전망된다. 글로벌 기업은 유망 중소기업을 인수 합병하여 기업규모를 키우고 정보보호 모든 분야로 사업을 확대하여 산업구조의 전문화 및 대형화 추세를 이어갈 것으로 예측된다. 최근 이종산업간 융복합화가 현실화되어 다양한 분야에 보안기능이 탑재되면서 융합보안 시장이 미래 블루오션으로 부상할 것으로 평가되고 있다.

국내 정보보호 시장은 KISA의 조사결과 2017년 87억불로 2012년 대비 약 2.1배 성장할 것으로 전망된다. 영상감시 및 바이오 인식은 무인감시, 출입통제 제품 분야를 중심으로 높은 성장률을 나타내고 있으며, 국가 주요시설뿐만 아니라 대기업 및 중소기업까지 APT 공격이 증가하고 있어서 성장세가 지속될 것으로 예측된다. 그러나, 국내 정보보호 시장 규모는 세계 시장규모의 2.4%에 불과하다. 이것은 국내 IT 시장 규모가 세계 시장 규모의 10% 수준인 것을 감안하면 매우 저조한 것이다. 특히 선진국은 정보보호서비스 중심으로 발전하고 있으나 국내는 여전히 정보보호 단위 제품 비중이 너무 높아 구조적인 측면

에서도 후진적 구조를 보여준다.

3. 우리 기술의 경쟁력

〈표 1〉에서 보는 바와 같이 주요국가 기술 경쟁력 수준에서도 우리는 미국에 비하여 1.8년 뒤지는 것으로 나타났다. 분야별로는 공통기반은 1.8년 네트워크 및 시스템 보안은 1.7년, 응용보안은 1.6년, 융합보안은 1.7년, 물리보안은 1.9년으로 조사되어 물리보안 기술이 상대적으로 격차가 큰 것을 알 수 있다.

표 1. 주요 국가별 기술격차(년)

구분	기술격차 (최고수준: 0년)
한국	1.8
미국	0
일본	1.1
유럽	0.7
중국	2.5

국내 기업들은 기초 및 원천 기술 부족으로 혁신적 신규 제품 개발보다 시장포화 상태인 기존 제품을 개선하는데 주력하고 있는 것으로 조사되었다. 또한, 국가차원의 연구개발 투자 측면에서도 미국은 국가전체 연구개발 투자액의 0.47%(7천억원)를 정보보호에 투자하지만 우리는 약 0.17%(288억원)를 투자하고 있어서 투자면에서도 매우 열악한 환경이다.

4. 주요 기술 동향

사이버 침해대응 분야에서는 행위기반 악성코드 분석기술에 대한 연구가 활발히 진행되어 왔으나, 여전히 신속하게 백신에 적용하는 것을 목표로 하고 있다 보니 APT 공격에 대한 입체적인 대응을 위한 연구개발은 초기수준으로 분석된다. 특히 공격자 추적을 위해서는 악성코드의 동작뿐만 아니라 프로그램으로서의 특징과 악성코드를 전파하는 과정의 특징, 악성코드가 이용하는 통신 프로토콜과 IT 자원들의 특성까지 분석하여 대응하는 것이 필요하다. 암호기술은 대용량 데이터를 암호화하고 복호화 하는데 걸리는 시간을 절약하기 위한 기술과 IoT 환경에서 이용할 수 있는 경량화 암호 기술, 동형암호와 같은 새로운 암호 기술에 대한 필요성이 증가하고 있다. 지능형 영상감시를 위해서는 영상 데이터에서 객체를 인식하여 추출하는 기술과 객체의 움직임에 따라 동작을 행위로 인식하는 기술이 필요하다. 이러한 기술의 특징은 응용의 요구사항에 따라 기술의 스펙트럼이 매우 넓기 때문에 원천기술과 응용기술을 분리하여 접근하는 것이 필요하다. 바이오 인식기술은 바이오 정보를 수집하는 과정에서 사용편의성을 제공하는 사용자친화형 바이오인식 기술의 요구가 증가하고 있으며, 바이오인식 기술이 서로 결합하여 인식률을 높이거나 응용분야를 확대하기 위한 연구들이 진행되고 있다.

Ⅲ. 목표 및 추진 전략

미래창조과학부가 정한 ICT 15대 미래서비스 중에서 정보보호 분야에 해당하는 서비스로는 사이버테러 실 실시간 대응서비스와 만리안 서비스가 있으며, ICT 10대 미래 기술 중에 정보보호 분야에 해당되는 기술은 사이버공격 대응기술이 있다. 사이버테러 실시간 대응서비스는 고도화된 사이버테러, 해킹, 악성코드 등에 대해 신속 탐지하고 대응하는 서비스로서, 사이버공격이 발생했을 때 공격으로 인한 피해 확산을 방지하고 공격방법을 조기에 분석하여 재발 방지를 위한 대책을 마련하도록 하는 것은 물론 공격 징후를 탐지하여 피해가 발생하지 않도록 예방하는 것까지 포함한다. 또한, 이러한 서비스는 단위 조직 내에서도 가능해야 하며 국가차원에서도 유효한 서비스가 되어야 한다. 만리안 서비스는 수 만개의 눈과 귀를 가진 스마트 CCTV 및 센서를 활용하여 범죄를 탐지하거나 예측하여 범죄율을 줄이는데 ICT 서비스를 적용하기 위한 서비스이다.

정보보호 기술 개발의 목표를 설정하는 과정에서 다음 세가지를 고려하였다. 첫째, 미래창조과학부의 15대 서비스와 10대 기술 개발 목표를 성공적으로 추진할 수 있도록 한다. 둘째, 국내외 시장 및 기술 동향에 부합해야 한다. 셋째, 기술 개발 결과가 가시적인 성과를 창출하여 정보보호 산업을 견인해 낼 수 있도록 한다. 이와 같은 고려사항을 토대로 정보보호 기술 개발 목표는 2013년 세계시장 점유율 2.4%에서 2018년 3.2% 달성하는 것을 목표로 설정하였고, 이를 위하여 10대 세계일류 제품을 선정하여 전략적으로 추진하기로 하였다.

1. 세계일류 제품

대한무역진흥공사에서는 2001년부터 매년 수출규모가 연간 5백만불 이상이거나 5천만불 이상의 시장규모인 제품군에서 시장점유율 5위 이내이면서 5%이상의 점유율을 차지하는 제품을 세계일류 제품으로 선정하여 발표하고 있다. 2013년 현재 441개의 세계일류 제품 중에서 정보보호 제품은 시큐어 OS, 온라인 게임보안 SW, 지문인증 모듈, DVR 카드, DRM 솔루션, 지문인식보안시스템 등 6종이 선정되어 있다.

2. 10대 세계일류 제품

2014년 기술개발 목표를 설정하기 위해 선정한 10대 세계일류 제품은 국내 기술 수준과 시장 특성을 분석하여 수출 주도형, 수입 대체형, 미래 성장형으로 분류하여 분류하였다. 수출 주도형은 내수중심 제품 군을 수출을 확대하는 전략에 해당하는 제품군이며, 수입 대체형은 글로벌 경쟁제품으로부터 국내 시장 잠식을 방어하기 위한 제품군이며, 미래 성장형은 원천기술을 확보하여 세계 신시장을 준비하기 위한 제품군이다.

표 2. 10대 세계일류 제품

구분	10대 세계일류 제품	목표제품/국가
수출 주도형	능동적 사이버 공격대응	FireEye/미국
	사이버 블랙박스	IBM QRadar/미국
	지능형 영상감시	ObjectVideo/미국
	유해콘텐츠 차단	McAfee/미국
	사용자 친화형 바이오 인식	L1 Identity/미국
수입 대체형	무선 침입탐지	에어타이트, 에어디펜스/미국
	산업용 통합 보안	Tofino/미국
	스마트 단말보안	ARM/미국 Infieon/독일
미래 성장형	동형 암호모듈	IBM/미국
	스마트 인증	RSA/미국

〈표 2〉에서 수출 주도형 제품군인 능동적 사이버 공격대응 제품은 새로운 사이버 보안 위협을 탐지하고 실시간 대응하기 위한 제품으로 행위기반 악성코드 분석 기술을 포함하여 최근 새로운 유형의 스크립트를 이용한 악성코드 유포 등에 대응하기 위한 제품이다. 사이버 블랙박스는 항공기 블랙박스나 자동차 블래박스와 같이 사고가 났을 때 각종 기록이 담겨진 블랙박스로부터 사고 경위를 조사할 수 있는 것처럼 사이버 환경에서도 사고의 원인을 조사 분석할 수 있는 증거 데이터를 저장 관리하는 장치와 이러한 장치의 데이터를 효과적으로 분석할 수 있는 기술을 포함한 제품이다. 따라서 데이터의 무결성 지원은 물론, 사후에 효과적으로 분석할 수 있도록 대용량 데이터를 관리하는 기술을 포함하며, 블랙박스 내의 정보가 확인된 사이버 사고와의 연관성이 있는지 여부를 수시로 분석할 수 있는 기술도 포함된다.

지능형감시 제품은 CCTV 및 각종 센서들로부터 상황정보를 수집하여 분석할 수 있는 제품으로서 통합관제센터에서 각종 범죄를 예방하거나 범죄 사실에 대한 증거를 수집할 수 있는 제품이다. 이는 대용량 영상 데이터로부터 객체를 추출하여 상황을 인지할 수 있는 능력과 각종 센서들의 상호 작용을 제어하고 연관성을 분석하는 기술들을 포함한다. 유해 콘텐츠 차단 제품은 성인용 유해 콘텐츠로부터 아동들을 보호할 수 있는 제품이다. 이것은 최근 보편화된 스마트폰 환경에서 실시간으로 동작하는 기술과 회피하는 것을 방지할 수 있는 기술을 포함한다. 사용자 친화형 바인오 인식 제품은 다중 스펙트럼 카메라처럼 사용자의 협조 없이도 복수의 바이오 정보를 획득할 수 있는 것처럼 바이오 정보가 ICT 환경에서 이용될 때 사용자의 거부감을 최소화 하면서 인식률을 높일 수 있는 제품이다.

수입 대체형인 무선 침입탐지 제품은 무선랜 환경에서 허가되지 않은 접속을 탐지하여 차단하는 기술과 데이터에 대한 기밀성을 제공하는 제품이다. 산업용 통합 보안 제품은 SCADA와 같은 산업제어 시스템 환경에서 동작하는 보안 제품으로 침입 탐지 및 차단은 물론 비정상 트래픽을 모니터링 하는 기술을 포함한다. 스마트 단말보안 제품은 스마트폰 내에서 정보처리에 대한 안전 신뢰성을 제공하는 기술로서 스마트폰용 보안칩과 칩환경에서 동작하는 보안 OS를 포함한다.

미래 성장형인 동형 암호 모듈은 대용량 데이터 처리시에 암호화된 상태 그대로 원문 정보에 대한 연산이나 검색이 가능하게 하여 데이터 처리 속도는 높아지고 외부 유출로부터 데이터 안전성을 지킬 수 있는 기술이다. 스마트 인증은 패스워드와 공인인증서를 대체하면서 입는 컴퓨터와 같은 모바일 환경에서도 활용 가능한 인증 인프라 기술이다.

3. 연도별 제품개발 로드맵

〈표 3〉은 연도별 제품 개발 계획을 나타낸다. 수입대체가 크거나 현재 기술 수준이 높은 제품은 단기적으로, 기술난이도가 높거나 미래 성장형의 경우는 장기적으로 목표를 설정하였다. 〈표 3〉과 같은 계획으로 제품 개발을 위해서는 2014년에는 기존 진행되고 있는 기술개발과제를 포함하여 모두 8개 제품에 대한 연구개발을 착수해야 할 것으로 분석된다.

표 3. 연도별 제품 개발 계획

년도	연도별 개발 제품
2014	무선 침입 탐지
2015	능동적 사이버공격대응 스마트 단말보안 유해콘텐츠 차단
2016	사이버 블랙박스 산업용 통합 보안
2017	지능형 영상감시 사용자 친화형 바이오인식
2018	스마트 인증 동형암호 모듈

4. 2014년 추진 방향

2014년 연구개발을 위해 정보보호 분야로 접수된 기술수요는 모두 75건이었다. 이들 중에 과제 내용이 유사한 것을 모아 36건의 과제로 다시 정리하여 전문가들이 참여하는 과제 기획 위원회를 통하여 추진할 과제를 최종 선정할 계획이다. 10대 세계 일류 제품 개발을 위해서는 과제기획 단계에서부터 기술개발, 특허, 표준을 연계하여 연구개발 성과의 시장선점 및 확산을 고려할 계획이다. 또한 성과 극대화를 위하여 산학연 수요처를 연계하여 중대형 과제기획을 추진할 예정이며, 이를 위하여 민간기업 협의체를 구성 운영하고, 보안관제, 컨설팅 등 기존 정보보호 서비스에 활용하거나 신규 보안 서비스를 창출할 수 있는 제품개발을 추진할 계획이다. 또한, 성과확산을 위하여 과제별 상용화 자문위원회를 운영할 예정이다.

Ⅳ. 결론

모든 것이 연결되는 초 연결 스마트 시대에 스마트플랫폼 기반으로 일상 생활 전 영역에서 ICT에 대한 의존도가 심화되어감에 따라 사이버 보안도 지속적으로 중요도가 높아지고 있다. 이러한 시점에 우리나라가 세계적으로 사이버 세상의 리더쉽을 확보하기 위해서는 정보보호 산업의 육성이 절실히 필요하고 이를 지원할 수 있는 기술 개발이 매우 중요하다. 이를 위하여 10대 일류제품을 계획대로 개발한다면, 어느 나라보다 보안이 골치거리인 우리가 보안으로 먹고 사는 나라가 되고, 그리고 국토는 좁지만 사이버 영토는 가장 넓은 나라를 만드는 데에 기여할 수 있을 것으로 기대한다.

약 력

원 유 재

1985년 충남대학교 이학사
1987년 충남대학교 이학석사
1998년 충남대학교 이학박사
1987년~2001년 한국전자통신연구원 무선인터넷 정보보호연구팀장, 책임연구원
2001년~2004년 안랩유비웨어 연구소장
2004년~2013년 한국인터넷진흥원 인터넷침해대응센터 본부장, 경영기획본부장
2013년~현재 한국산업기술평가관리원 정보보호 CP
관심분야: 정보보호, 인터넷보안, 시스템보안

이 태 진

2003년 POSTECH 컴퓨터공학과 공학사
2008년 연세대학교 컴퓨터공학과 공학석사
2013년~현재 순천향대학교 정보보호학과 박사과정
2003년~현재 한국인터넷진흥원 정보보호기술개발팀 책임연구원
관심분야: 악성코드 탐지 및 분석, 네트워크 보안

문 기 영

1986년 경북대학교 전자공학과 공학사
1989년 경북대학교 전자공학과 공학석사
2006년 충남대학교 컴퓨터과학과 이학박사
1992년~1994년 대우정보시스템 기술연구소 전임연구원
2010년~2011년 캘리포니아 주립대 초빙연구원
1994년~현재 한국전자통신연구원 영상보안연구실 책임연구원
관심분야: 영상보안, 바이오인식, 웹 보안