제1호 발로뛰는 중소기업 호민관

국회의원 정태근

『중소기업을 살린다』
국정감사 자료집 제 10 호

지식정보보안 산업 살린다!

– 인터넷, 스마트폰, 웹뷰어 등 사이버세상은 더 이상 안전지대가 아니다.

2010. 10.

국회 지식경제위원회

국회의원 정태근

< 목 차 >

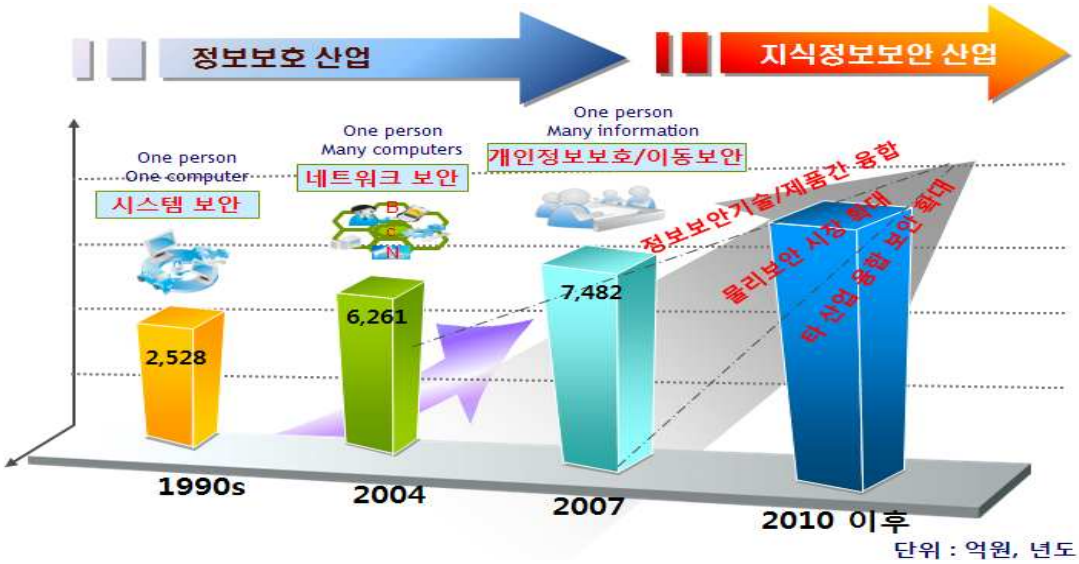
I. 지식정보보안산업 개요

1. 지식정보보안산업의 정의

□ 지식정보보안은 암호, 인증, 인식, 감시 등의 보안기술이 적용된 제품을 생산하거나, 관련 보안기술을 활용하여 재난·재해·범죄 등을 방지하는 서비스를 제공하는 기술 산업

o 새로운 정보통신기술의 개발과 다른 정보통신 관련 역기능 및 신종범죄의 발생으로 필수불가결하게 지식정보보안산업이 발전

o 세계 IT보안 산업의 트렌드가 '통신상의 정보보호'에서 '개인 및 사회 안전'으로 빠르게 진화하면서 유비쿼터스 사회 진입에 따라 정보보안의 개념이 컴퓨터 및 네트워크 수준의 보안을 넘어 사회 전반의 보안으로 확장



[그림 6] 지식정보보안산업의 발전 예상도

□ 미국, 유럽, 일본 등에서 차세대 성장 동력으로 지목하고, 국가 차원에서 적극적으로 집중 지원 및 육성 중

2. 지식정보보안산업의 특성

□ 국가·개인·기업의 유·무형 자산 및 인적자원에 대한 안전과 보호를 위한 공공성이 큰 지식정보 인프라 산업

o 미국은 9.11테러 이후 정보보안 및 보안·경비 산업이 급속도로 발전하고 있으며 미래유망 산업으로 부상

o 불법·유해정보 유통방지, 지능형 감시 등 클린 인터넷 경제 및 국가사회 안전망구축에 기여

o 보안사고 예방으로 인한 경제 외부 파급효과(ROSI)가 큰 산업
- 사례 : 지난 '03년 1월 25일 침해사고 시 1,630억원의 GDP 손실액 발생
*** 출처 : 지식정보보안산업의 이해, 지경부**

□ 국가 안보 보장, 타 산업 활성화를 위한 인프라로서 중요할 뿐만 아니라 그 자체로서도 성장 가능성이 높은 산업

o 네트워크 사회로 발전함에 따라 사회경제시스템 전반에 대한 안전과 보호가 더욱 절실히 요구되는 상황

o 보안사고로 인한 막대한 경제적 손실을 예방하고, 전력망 등 기간산업보호, 전자금융안전거래 등 경제활동 기반 안정화 실현

□ 시장 성장성과 수출 잠재력이 높은 신 성장 산업

o 보안 산업의 트렌드가 '통신상의 정보보호'에서 '개인 및 사회안전'으로 빠르게 진화함에 따라, 중점분야도 방화벽, Anti-virus, Anti-spam 등의 시스템·네트워크 보안에서 스마트폰 보안, 지능형 카메라, 스마트그리드 보안 등 사회 안전 및 시설 보안으로 변화

[그림 7] 지식정보보안산업의 현황 및 특징

o 세계 지식정보보안산업은 최근 3년간 연평균 12.7%의 고성장

* 과거 3년간 6.2% 성장한 IT산업 대비 2배 이상 고성장
* 선진국 기업은 차별화된 보안기능을 마케팅의 중요 전략으로 활용

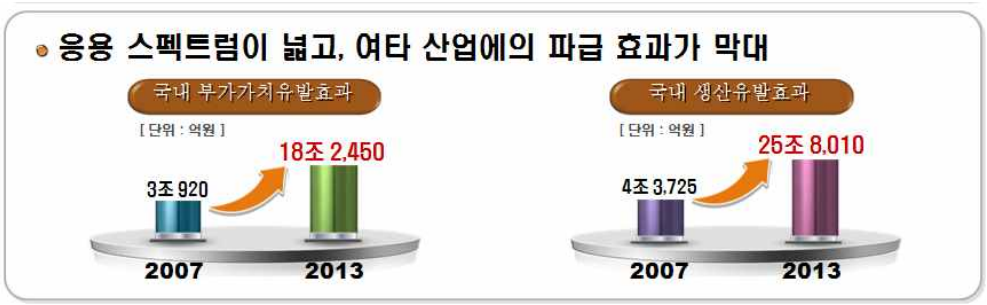
[그림 8] 지식정보보안산업의 시장 예상 규모

* 출처 : 지식정보보안산업 진흥 종합 계획, 지경부

□ 응용 스펙트럼이 넓고, 타 산업에의 파급 효과가 큰 산업

o 전통적인 시스템 및 네트워크 보안에서 콘텐츠, 자산, 시설 보안으로 산업 영역이 확대되면서 부가가치 및 생산유발효과 양산

* 생산유발효과 : 4조 3,725억원('07) → 25조 8010억원('13)
* 부가가치유발효과 : 3조 920억원('07) → 18조 2,450억원('13)



[그림 9] 지식정보산업의 파급 효과

*** 출처 : 지식정보보안산업 진흥 종합 계획, 지경부**

□ IT보안, 즉 정보보안 기술은 통신 환경에 따라서 PC보호, 네트워크 통신, 방송, 네트워크 및 서비스 기술이 융·복합 되는 유비쿼터스 환경으로 진화하고 궁극적으로 물리보안 및 정보보안 기술과 전통 산업간 융합으로 창출되는 융합 산업보안 기술로 발전 예상

II. 지식정보보안산업 동향

1. 사이버 보안 위협 동향

□ ’10년 상반기는 DDoS 공격이 35.4%로 가장 많고, 그 다음으로 웹사이트 공격(34.8%)으로 분석

o 공격 양상은 공격 기법의 진화, 공격 범위의 확대, 대범한 범죄화, 사이버 암시장 형성에 따른 대중화로 나타남

o 악성코드 탐지 및 차단 건수는 약 6,570만 건에 달해 ‘09년 하반기 대비 144만 건(2.2%)이 증가

*** 출처 : ‘10년 상반기 보안 위협 동향, 안철수 연구소('10)**

□ 기업을 겨냥한 표적 공격 위협의 증가

o 기존의 전방위적인 무작위 공격에서 특정 기업을 조준한 표적 공격으로 있는 추세

o ’09년 말 ‘하이드락 트로이목마(Hydraq Trojan)는 특정인을 속이는 방법인 사회 공학적 기법을 이용하여 표적 기업의 핵심정보에 접근

□ 공격용 툴킷의 보편화로 사이버 범죄 급증

o 초보자들도 손쉽게 시스템을 공격하고 정보를 빼돌릴 수 있는 악성코드를 만들 수 있게 되면서 사이버 범죄가 급증

*** 개인정보 탈취하도록 설계된 악성코드를 자동 생성하는 제우스(Zbot)는 700 달러 내외에 구입 가능**

o 제우스와 같은 툴킷을 이용해 수백만개의 악성코드 변종 생산 가능

□ 웹 기반 공격의 지속적인 증가

o ’09년 PDF뷰어를 겨냥한 웹 기반 공격이 전체의 49%로 급증, ‘08년 11% 대비 기록적인 증가 추세

*** 출처 : http://www.symantec.com/ko/kr/about/news/release/article.jsp?prid=20100421_01, 시만텍**

□ 아이폰과 안드로이드 모바일 플랫폼의 공격 증가

o 스마트폰을 대상으로 한 위협이 통화 기록이나 전화번호, 사진 등의 개인 정보 탈취 위협 증가

o 스마트폰을 좀비 클라이언트로 만들어 DDoS 공격에 악용 가능성 존재

□ 신흥국가, 악성 활동 주요 국가로 부상

o 브라질, 인도, 폴란드, 베트남 및 러시아 등 IT 인프라 및 광대역 통신망이 빠르게 발전하고 있는 신흥 국가에서 악의적 활동들이 급증

o 이는 선진국들의 강력한 사이버 범죄 규제로 인해 범죄자들이 관련 법규제가 상대적으로 느슨한 개발도상국으로 본거지를 옮기고 있기 때문인 것으로 풀이

□ 잠재적 사이버 위협 상존

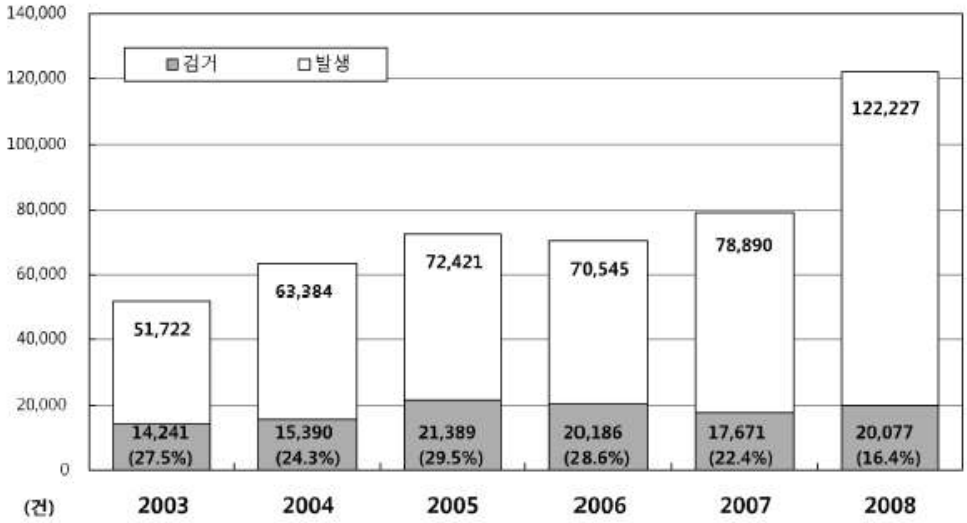
o '09년 말 현재 전 세계적으로 약 650만대의 컴퓨터가 컨피커 웜에 감염되어 있는 것으로 파악

o 컨피커 웜의 배후 범죄세력이 여전히 감염된 컴퓨터에 대한 키를 보유하고 있기 때문에 언제 터질지 모르는 시한폭탄과 같음

o '09년 2억4천만 개 이상의 새로운 악성 프로그램이 탐지되었으며, 이는 '08년과 비교해 100% 증가한 것으로 분석

*** 출처 : 인터넷 보안 위협 보고서, 시만텍**

□ 국내 사이버 공격 발생건수는 '07년 78,890건에서 2008년 122,227건으로 65% 증가하였으나, 사이버 공격의 다양화와 복합화 등으로 인해 발생 대비 검거 건수는 '07년 22.4%에서 16.4%로 줄어듦



[그림 10] 사이버공격 발생 추이

* 출처 : 경찰청 사이버테러대응센터(NETAN),('09), http://ctrc.go.kr

2. 국내·외 지식정보보안 시장 동향

□ 세계 지식정보보안산업의 시장 규모는 '08년 기준, 2,018억불로 연평균 약 12.7%대의 높은 성장률을 기록

o 물리보안 및 융합보안 시장의 성장세에 힘입어 '13년경 지식정보보안산업의 시장은 3,680억불 규모로 증가할 전망

구 분	2007년	2008년	2009년	2010년	2011년	2012년	2013년	CAGR
총 액	416	476	545	633	725	825	982	15.39%

[그림 11] 국외 지식정보보안산업의 전망

* 출처 : 세계 지식정보보안 시장 전망, IDC('08)

□ 미국과 EU 등 2개 지역이 전 세계시장의 88%를 점유하는 전형적인 글로벌 독과점산업이며, 일본과 이스라엘이 나머지 시장을 분할

o 시장점유율(%) : 미국(51.2), EU(37), 일본(5.7), 이스라엘(4.1), 한국(1.7)
*** 출처 : 지식정보보안 R&D 발전전략, 한국산업기술평가관리원('10,5)**

□ 그간 정보보안을 중심으로 산업이 성장해 왔으나, 최근 물리보안 및 융합보안 분야가 新성장축으로 부상하며 산업성장을 주도

o 미국은 시만텍, 시스코, 오라클 등 글로벌 보안 기업을 앞세워 정보보안 산업에서 전 세계 시장의 45%를 점유, 시장을 주도
*** 시스코, 주니퍼 : 네트워크 보안, MS, 오라클 : OS보안, IBM, HP : 서버보안**

o 특히, 시만텍 등 글로벌 정보보안 기업들은 M&A 등을 통해 대형화·전문화 및 사업 다각화를 추구
*** 시만텍, ISS/체크포인트, RSA : 공격적 M&A로 경쟁력 확보 및 사업다각화**

o EU는 전 세계 물리보안 시장의 55%를 점유함으로써 세계 최대의 보안장비 생산지이자 소비지로 부상

o 향후 기존의 물리보안 제품에 네트워크 기술이 접목된 IT기반 물리보안 제품이 성장을 주도할 것으로 예상

o 또한 유비쿼터스 사회에서 차량, 국방, 의료, 건설, u-물류·항만 시스템의 안전과 신뢰성을 담보하는 핵심요소로 시장수요 급증 예상

□ '07년 국내 시장은 약 3조 1천억원으로 세계시장 대비 1.74% 수준
*** 출처 : 지식정보보안 R&D 발전전략, 한국산업기술평가관리원('10,5)**

□ 국내 지식정보보안 업체는 약 590여개이며 이중 지식정보보안 업체의 약 60%는 자본금 6억원, 종사인력 30명 이하의 영세한 기업으로 구성
*** 출처 : 지식정보보안 R&D 발전전략, 한국산업기술평가관리원('10,5)**

o 네트워크 보안장비(시만텍, 시스코 등)등 고가의 HW제품은 대부분 수입에 의존하고 있고, 방화벽이나 바이러스 백신 등 SW제품 위주로 일본, 미국 등에 수출

o 국내 시장에서 외산 제품이 차지하는 비중은 약 9.1% 수준

* '07년 기준으로 수입액(618억원)이 수출액(532억원)을 약간 초과하였고, 일본(55.9%), 미국(19.4%), 중국(16.4%) 등이 우리나라의 주요 수출국에 해당

[그림 12] 정보보안 제품 수출입 규모

* 출처 : 지경부 '지식정보보안산업 진흥 종합계획' 발표('08.12)

3. 국내·외 지식정보보안 기술 동향

□ 지능화, 복합화, 조직화되고 있는 사이버 공격 기술의 발전 추세에 따라 네트워크・시스템 보안 기술도 고도화, 통합화, 능동화, 선제적 대응화되는 추세

o 네트워크의 가용성을 저해하는 DDoS 공격 대응, 악성코드에 대한 근원적 대응을 위한 지능형 DDoS 공격 대응 및 악성코드 분석기술 개발과 모바일 단말의 임의조작방지 및 보호를 위한 보안 플랫폼 개발에 집중함

o 통신망 융복합화, 사이버공격 고도화 환경에서 네트워크・시스템 보호를 위한 모바일 단말 플랫폼 보안, 지능형 악성코드 자동분석, 클라우드 컴퓨팅 보안, 고성능・응용계층 DDoS 탐지・대응, 신종 봇넷 탐지 등 사이버 공격 조기 탐지・차단・대응 기술

<표 1> 국내외 기술 개발 동향

구분	현재 기술(~에서)	개발 방향(~로)
네트워크 침입대응	- 개별 기능 단품형 솔루션에서	- 다기능 통합형 솔루션으로
	- DoS 및 DDoS 대응에서	- 지능형 고성능 DDoS 대응으로
악성코드 대응	- 네트워크기반의 시그니처 분석 탐지에서	- 네트워크기반의 이상 행위 탐지 및 능동형방어로
	- IRC,HTTP 봇넷 대응에서	- 신종(P2P 등) 봇넷 능동형 탐지 및 대응으로
보안운영체계	- PC/서버용 보안 플랫폼에서	- 모바일용 임베디드 보안 플랫폼으로
디지털포렌식	- 컴퓨터 및 모바일 포렌식에서	- 포렌식 도구 기능 검증으로 - 안티 포렌식 대응으로
보안 전용 칩셋	- 고속 보안 칩셋에서	- 경량, 저전력 보안 칩셋으로
접속보안	- 수 Gbps급 보안 장비에서	- 수십 Gbps급 보안 장비로
	- 동종 망간 보안 연동에서	- 이종 망간 보안 연동으로
보안 관리	- 단위망 보안관리에서	- 전역적 중앙집중식 보안관리 체계로
	- 보안장비의 단순 통합관리에서	- 네트워크 장비를 포괄하는 연계 제어로

<표 2> 표준화 동향

구분	국외 동향	국내 동향	대응 전략
네트워크 침입대응	-유무선 네트워크 환경에서의 역추적 요구사항 정의와 다중 도메인간 협업형 역추적 프레임워크에 대한 표준화 진행중	-보안장비의 보안이벤트 로그 포맷 이외에도 보안관점의 네트워크 트래픽 현황에 정형화된 형식에 대한 표준화 진행중	-향후 역추적기술의 프레임워크 및 메커니즘에 대한 표준화 추진 필요
악성코드 대응	-ITU-T SG17에서 봇넷 탐지 및 대응 프레임워크와 봇넷을 이용해 발송되는 스팸 대응 수단에 대한 표준화 추진	-TTA PG503에서 봇넷 대응에 관한 표준화 진행중	-봇넷 관련 국제표준화 활동이 미비하기 때문에 기술개발 초기부터 표준안 개발 추진을 통한 관련분야 시장성 및 주도권 확보 가능
디지털 포렌식	-ISO/IEC JTC1/SC27에서 디지털 포렌식 관련 신규 표준화 과제 추진 -ITU-T SG17에서 사이버 범죄 추적 및 디지털 증거 파일 교환 포맷과 관련된 표준화 진행	-디지털 증거 수집 과정 및 명문화 절차에 관한 표준화 활동 미비 -2007년부터 TTA를 통해 디지털 포렌식 가이드라인 및 수집·분석도구 검증을 위한 표준화가 진행	
접속보안	-ITU-T, IETF, ISO/IEC JTC1 등에서 네트워크 보안 기술 표준 활동 -3GPP를 중심으로 IMT-Advanced 기술에 대한 표준화가 활발하게 추진 -무선랜에서 발생할 수 있는 보안 문제점을 해결하기 위해 IEEE와 IETF가 상호 협력하여 표준화 진행	-BcN 보안분야는 다양한 프로젝트 그룹 및 워킹그룹이 형성되어 표준화 진행 -TTA에서 와이브로 네트워크에서의 IPv6 기술 적용 표준화 추진 -TTA TC5 및 TC3에서 모바일 단말 관련 보안표준 추진 예정	-유무선 통합보안 기술에 조기 기술개발 및 표준화 추진 필요
보안관리	-침해사고 정보교환 포맷과 전달 프로토콜에 대한 표준이 있으며, 역추적기술의 프레임워크와 메커니즘에 대한 표준화가 추가적으로 진행	-보안기술포럼과 TTA에 의해 사이버 공격 역추적 및 보안관리 일반 표준 추진 -멀티 도메인간 협업 기반의 사이버공격 역추적 보안이벤트 포맷 및 프레임워크에 대한 표준화 완료	-효율적인 보안관리 가이드라인 제공을 위해 직관적인 보안관리 인터페이스에 대한 표준화 필요

<표 3> 특허 동향

구분	국외 동향	국내 동향	대응 전략
네트워크 침입대응	-수동형 공격뿐만 아니라 능동형 공격을 막기 위한 여러 기법들(공격 패턴에 기반을 둔 탐지, 새로운 공격에 대한 탐지 기법) 등을 중심으로 지속적인 특허 출원	-여러 개의 탐지 기법을 동시에 사용하는 하이브리드 기반 탐지 기법을 제안하는 특허가 출원 되고 있음	-변종과 같은 새로운 형태의 공격에 대응할 수 있는 기술 개발 및 특허 필요
악성코드 대응	-바이러스 변종 피해가 증가하면서 이를 탐지하기 위한 기법을 중심으로 특허가 출원되고 있음	-기본 PC 환경뿐만 아니라 모바일 환경에서 발생 할 수 있는 악성코드를 탐지하기 위한 관련 특허가 출원되고 있음	-IRC/HTTP 봇넷 관련 네트워크 기반의 탐지 기술에 대한 특허 확보에 주력
디지털포렌식	-컴퓨터 포렌식 분야는 미국이 현재 가장 많은 특허를 보유, 모바일 및 네트워크 포렌식 분야는 미국, 유럽, 일본 등이 비슷하게 특허를 보유	-컴퓨터 포렌식을 중심으로 한 특허 중 우리나라는 약 20%의 관련 특허를 출원 중이며, 향후 e-Discovery 분야 특허가 활발해질 것으로 전망	-e-Discovery 분야의 특허 확보를 위한 전략 필요
접속보안	-아직 4G 관련 보안 기술의 특허 출원은 미비한 수준이며, 이동 단말의 보안기술, 멀티미디어 서비스 응용 보안기술, 망간 연동을 위한 보안기술이 대부분을 차지	-통신망간 연동 보안 특허, 이동 단말의 USIM 관련 특허, 모바일 뱅킹 등 이동통신 보안 응용 서비스에 대한 특허가 활발히 출원되고 있음	-4G 관련 보안기술 개발 및 핵심 특허 확보를 통해 국제적 기술 선점 필요
보안 관리	-미국은 이벤트 시각화 분석기술, 트래픽 Flow 또는 Netflow 기반 분석 기술, 취약성 분류 기술에 강점을 갖고 일본은 모든 부분에서 미국과 한국에 비해 특허 출원이 적음	-네트워크 침입 흔적 추적 기술도 미국과 일본보다 강점을 가지고 있지만, 반면 Event / Log Correlation 기반의 분석 기술은 미국과 일본에 비하여 취약함	-국외에 비해 상대적으로 취약한 Event / Log Correlation 기반의 분석 기술에 대한 대응 특허 확보 필요

* 출처 : 지식정보보안 R&D 발전전략, 한국산업기술평가관리원('10,5)

□ OS, 네트워크 보안에 대한 기반기술이 열위이며, DB보안, 콘텐츠 보안 등 일부기술력 보유

* 기술격차(년) : 미(0), EU(1.7), 일본(2.6), 한국(3.3), 중국(6.2)

[그림 13] 정보지식산업 기술력 비교

* 출처 : 지경부 '지식정보보안산업 진흥 종합계획' 발표('08.12)

4. 국내·외 지식정보보안 정책 동향

□ 美國 국토안보부(Department of Homeland Security)는 '10년 사이버보안 예산으로 '09년 대비 13% 증액한 3억5,500만달러(약5,559억원) 요구

*** 09년 예산 : 3억1,350만 달러(4,900억원)**

o 국가의 공공·민간의 정보네트워크 보안에 집중적인 투자 및 국가 사이버보안계획 (CNCI, Comprehensive National Cyber security Initiative) 참여 강화

*** CNCI : 미국내 인터넷 위협 탐지기술 개발 및 사이버공격 방어능력 개선을 위한 계획으로, 개발 중인 기술들은 향후 5~10년 내에 활용 예상**

o 예산 요구액 중 3천6백만 달러(약 564억원)는 고도화된 생체무기의 위협을 탐지하기위한 기술개발 프로젝트에 투입

*** 국토안전부는 '09년 사이버보안 예산의 많은 부분은 사이버위협 및 침입 분석을 위한 Einstein 구축에 투입**

*** 출처 : 지식정보보안 R&D 발전전략, 한국산업기술평가관리원('10,5)**

□ 국가 최상위 수준의 사이버보안리더십 발휘 및 총괄조정 기능 강화를 위해 오바마 美대통령이 백안관 기자회견을 통해 '사이버스페이스 정책 리뷰(Cyberspace Policy Review)' 연설('09.5.29)

o 경제성장, 시민의 자유와 프라이버시 보호, 국가안보, 민주 제도 개선을 위해 사이버 보안을 행정부의 국정 우선순위로 설정

o 백악관에 사이버보안 정책관 직위를 신설하여 연방정부의 사이버 보안 정책을 조정하고 통합하는 역할을 담당

o 정보통신 관련 법률 통합 및 체계화, 의회와의 공고한 협력 관계 유지

o 연방정부의 사이버보안 선도 및 책임성 강화, 행정부처, 주정부 리더들의 책임 있는 자세 강조

□ '에너지 자립 및 안전 법안'에 스마트 그리드 관련 내용을 포함하고, '09년 경기부양 법안에 540억 달러의 투자를 명시

o 스마트그리드 사이버 보안 투자 예산은 전체 스마트그리드 투자금액의 15%에 해당될 것이라고 추정

*** 출처 : Pike Research, Smart Grid Security Market('10)**

o '09년~'15년 동안 전 세계 스마트그리드 사이버 보안 시장은 20% CAGR로 성장할 것으로 전망

* '09년 스마트그리드 사이버 보안 시작은 12억달러로 추정
* '13년 41억달러로 예상, ' 15년에는 37억달러로 전만됨(출처 Pike Research)
* CAGR(Compound Annual Growth Rate) : 연평균 성장률
* 출처 : 지식정보보안 R&D 발전전략, 한국산업기술평가관리원('10,5)

□ EU는 디지털 경제성장의 핵심을 미래 인터넷으로 전망, 미래인터넷 환경조성을 위한 구체적인 실현방안 발표('08.9)

o EU 집행위원회는 경제회복 대책의 일환으로 '10년까지 초고속인터넷 구축에 10억 유로 (약 1조8천억) 투자 결정('09.1)

* 미래 지향적인 인터넷 아키텍처 구축, 무선 인터넷 서비스 활성 강화
* 기하급수적으로 증가될 인터넷 이용을 대비하여 이용자의 정보 및 개인정보 보호 투자 강화 등
* 출처 : 지식정보보안 R&D 발전전략, 한국산업기술평가관리원('10,5)

□ 일본 經産省은「신IT개혁전략 (안전·안심의 정보사회 환경조성)」으로 정보보안 기술개발에 44.9억엔 투자

* 삶의 질 개선을 위한 과학기술 혁신 전략으로「재해 정보통신시스템 기술」 R&D에 41억엔 투자('08)
* NISC(국가정보보호센터) 설립하여 정보보호 영역확대에 따른 보안융합 원천기술 개발 및 기초연구 강화
* 출처 : METI(Ministry of Economy, Trade and Industry, 일본 경제산업성, '06)

□ 국내 지식경제부에서는 지식정보보안산업 발전전략을 수립하여 기존의 정보보안, 물리보안, 융합보안 등 지식정보 보안 산업 3대 핵심 분야의 신기술 개발 및 사업화 촉진을 통해 지식정보보안시장을 '18년까지 20조원 규모로 육성 계획 추진을 위한 『Securing Knowledge Korea 2013』 발표

* 출처 : 지식정보보안산업 진흥 종합계획 발표, `08.12

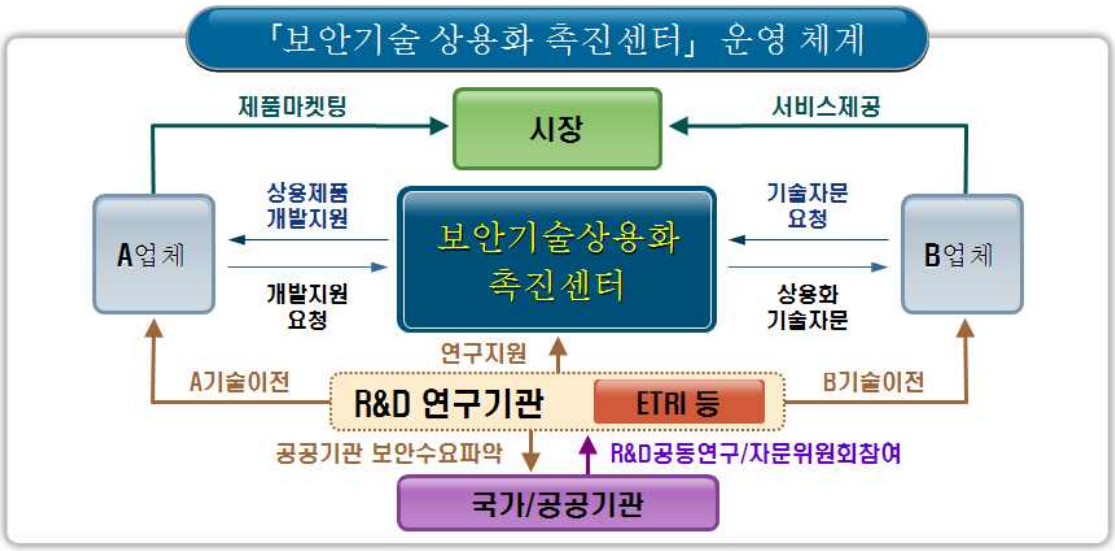
o 지식경제경부, 미래기획위원위(대통령 직속 기관) 및 방송통신위원회 공동으로 IT KOREA 5대 미래전략에서 미래 사이버 위협대비를 위해 연구 개발 및 산업 육성을 지원키로 보고('09.9)

o 지식경제부, 방송통신위원회, 행정안전부, 국가정보원 공동으로 '10년까지 제도개선 및 정보보호 인프라를 조성하여 지식정보보안을 위한 사회안전망을 구축하고, '12년까지 우리나라의 국제 정보보호 순위를 세계 5위로 끌어 올리기 위한「정보보호 중기 종합계획」수립·발표 ('09.7)

o 국방부는 급증하는 사이버위협에 체계적으로 대응하기 위해 국방정보본부 산하에 국방 사이버 지휘통제센터를 중심으로 인터넷 해킹 예방, 보안관제, 복구 등을 총괄 지휘 하는 사이버사령부를 창설('10.1)

o 국가사이버안전전략회의에서 사이버공격 차단·대응을 위한 기술개발 예산 및 보안산업 상용화를 위한 예산 증액지원 추진('09.9)

o 글로벌 역량 강화를 확보를 위한 중점보안기술 상용화 촉진



[그림 14] 보안기술 상용화 촉진센터 운영 체계

* 국가보안기술연구소 연구 성과물을 단계적으로 민간에 기술이전('09년~)
* "기술이전 거래장터"를 개설, 민간으로 기술 이전을 추진

* 출처 : 지경부 '지식정보보안산업 진흥 종합계획' 발표('08.12)

III. 사이버공격 피해사례

1. 국외 주요국의 사이버 공격 사례

<표 4> 국외 주요국의 사이버 침해사고 사례

날짜	사이버 침해사고 사례
'10년 6월	● 발전소·공항·철도 등 기간시설을 파괴할 목적으로 제작된 컴퓨터 바이러스인 Stuxnet 발견 - 美國, 이스라엘이 이란의 핵시설을 마비시키기 위해 퍼뜨린 사이버 무기라고 추정
'09년 3월	● 중국에 의한 주요 기밀 정보 외부 유출 - 동남아, 유럽 등의 주요 정부 기관 및 대사관이 Ghost라는 트로이목마에 감염으로 주요 기밀 정보들이 외부로 유출
'09년 1월	● 러시아 해커 키르기즈스탄 공격 - 러시아 사이버의용군이 키르기즈스탄의 대형 ISP에 대하여 DDoS공격으로 인터넷이 마비 ● 오바마 대통령, 브리트니 스피어스 등 33명의 유명 인사들의 트위터 계정 해킹
'08년 12월	● 반크 홈페이지 공격 - 일본 네티즌의 공격으로 반크사이트에 대한 해외 접속 불가
'08년 8월	● 러시아·그루지아 사이버전쟁 - 영토분쟁으로 무력충돌이 확산되고 있는 가운데 러시아 해커들에 의해 그루지아 국방부, 외교부 등 주요 사이트가 공격을 받음
'07년 4월	● 러시아 해커 에스토니아 공격 - 에스토니아 수도 '탈린'에 있던 구소련군 동상이 철거되자, 러시아 해커에 의해 대통령궁, 정부부처, 정당, 금융기관 등 대상 대규모 사이버테러 감행으로 행정업무 마비 등 국가적 혼란 야기
'07년 2월	● 루트 DNS DDoS 공격 - 루트 DNS 6개가 Virut 바이러스 감염 PC에 의해 DDoS 공격 피해 발생
'03년 7월	● 미국 7개주 정전 사태 - 블래스터 웜으로 국지적 정전사태가 7개주에 걸친 대규모 정전사태 확대로

2. 국내 사이버 공격 피해 사례

<표 5> 국내 사이버 침해사고 사례

날짜	사이버 침해사고 사례
'09년 11월	• 국내·외 주요 보안업체 홈페이지 잇단 해킹사고 발생
'09년 10월	• D 대학 졸업생이 해킹프로그램을 활용하여 관리자권한을 탈취하여 성적 조작
'09년 7월	• 청와대, 백악관 등 한미 주요 기관 웹 사이트와 일부 포털 등이 해커들의 DDoS 공격을 받아 다운되거나 접속장애 상태 발생
'09년 3월	• Conficker 변종 악성코드 감염으로 인한 피해 증가
'09년 2월	• IT 보안업체 위장 DDoS 공격 검거(협박성) - 보안전문가들이 보안업체를 설립한 후 해당 사 서비스를 이용하도록 하기 위해 Bot을 이용하여 DDoS 공격
'09년 1월	• ○○평가원 수능자료 등 주요 자료 유출 사고 발생
'08년 2월	• 해킹에 의해 옥션 이용자 1천 81만명의 개인정보 유출
'03년 1월	• '1.25 인터넷 대란'으로 윈도우 서버의 취약점을 이용한 '슬래머 웜' 바이러스에 의해 전 세계 7만5천대 및 국내 8천 800여대 컴퓨터가 감염

3. 사이버 공격에 의한 발생하는 피해

□ ’10년 7월 美 백악관의 사이버 정책 보고서에 따르면 ‘08년~‘09년 사이버 공격으로 인한 지적재산권 피해금액이 1조 달러에 달한다고 발표

□ 美 기업들이 해킹 등 사이버 범죄로 인해 연간 평균 380만달러(46억원 상당)의 손실을 입고 있다는 조사 결과 발표

o ’10년 7월 美 샌프란시스코 크로니클에 따르면 IT 보안업체인 아크사이트(ArcSight)가 기업 45곳의 데이터 등을 분석한 결과 이들 기업 45곳은 주당 50회 가량의 ‘성공적인’ 사이버 공격 피해를 받음

o 사이버 공격으로 인한 연간 피해액은 적게는 100만 달러에서 많게는 5천200만 달러에 이른 것으로 나타남

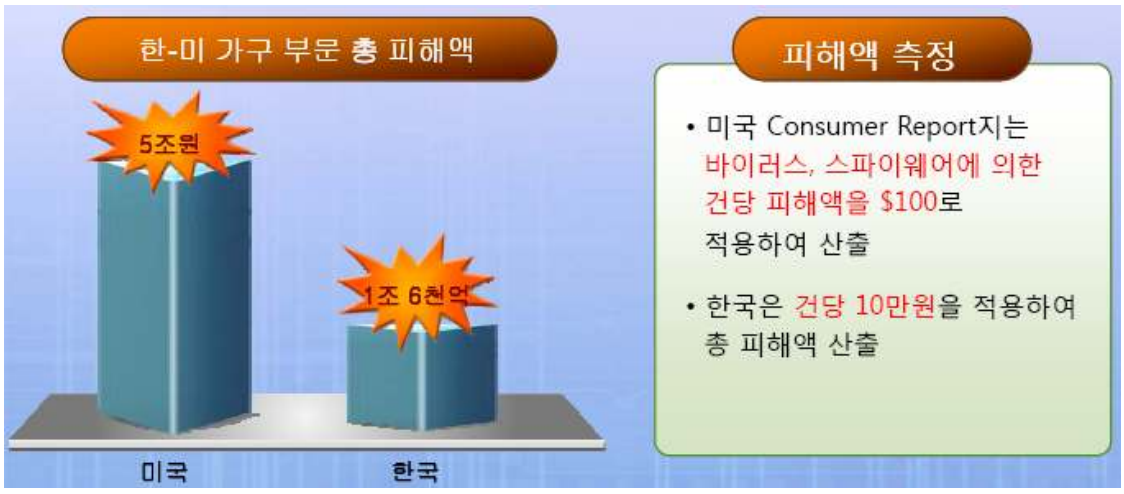
*** 출처 : 아크사이트 보고서**

□ 美 인터넷 이용 가구의 인터넷 침해사고 피해액은 약 50억 달러(5조원)

*** 출처 : 美 Consumer Report지가 미국 내 인터넷 이용 2,030 가구를 대상으로 실시한 설문 조사 결과**

□ ‘07년 미국과 같은 기준으로 측정한 우리나라 가구의 침해사고 피해액은 약 1조 6천억원

*** 출처 : 7.7 DDoS 공격 이후 정부 대책방향, 방송통신위원회(‘09.10)**



[그림 15] 사이버 공격으로 인한 경제적 손실

□ ‘09년 7월 발생한 7.7 DDoS 공격의 피해액이 최소 363억원에서 최대 544억원으로 분석

o ‘08년 국내 풍수해 피해액이 580억원임을 감안할 때 DDoS 공격으로 인한 피해가 적지 않음

*** 출처 : 현대경제연구원(‘09.7)**

IV. 국내 지식정보보안산업의 실태분석

1. 지식정보보안산업 SWOT

□ 강점(Strength)

o 인터넷 환경에서 세계 최고로 다양하고 고도화된 서비스 경험과 높은 보안성 유지를 위해 축적된 기술 및 경험 보유

o 유선 인터넷 서비스에서 발생되는 웹어플리케이션 공격 등 다양한 보안 위협에 대한 대응기술 수준 높음

□ 기회(Opportunity)

o 제2의 인터넷붐 조성을 위해 스마트폰 산업 활성화 정책 등 정부의 육성 의지가 강함

o 국가 기반 인프라의 정보보안 기술의 접목을 통한 국가 신뢰도 증대 가능

o 새로운 IT 융합 환경 도래 (정보보안 기반 기술을 다양한 응용 분야로 활용 가능)

o SNS 등 다양한 신규 융합 서비스 확산 이전 초기화 단계에서 사이버 역기능에 대한 사전 예방적 대응기술의 적용이 가능

□ 약점(Weakness)

o 암호, 인증 분야의 핵심 원천 기술에 대한 투자 부족

o 선진국에 비하여 지능형 영상인식 SW에대한 기술 경쟁력이 미흡

o 정보보안 업체의 영세성으로 인해 고급기술개발을 등한시하여 경쟁력 저하

o 지식정보보안 원천 및 핵심 기반 기술 미흡

o 국가 기반 인프라에 대한 보안 및 안전성 미흡

o 개인정보 및 자산보호에 대한 인식 미흡

o 지식정보보안산업 활성화를 위한 기반 법·제도 미흡

o 무선 인터넷서비스 대상의 보안기술은 유선 보안기술 대비 상대적으로 미흡

□ 위협(Threat)

o 모바일 환경으로의 전이과정에서 국내 보안 기술이 경쟁력을 상실할 위험이 있음

o 정보보안과 타산업의 결합으로 인한 위협 요소 증대

2. 지식정보보안산업의 육성책 미흡

□ 정부의 정보보호 총괄기능의 분산 및 민간부문 정책부서 축소

o '08년 정부 조직개편에 따라 정보보호 정책기획 기능이 방송통신위원회, 행정안전부, 지식경제부 등으로 분산됨에 따라 사건 발생 후 해당 사안을 주도적으로 관장하는 기관이 없었음

□ 전체 정보보호대상의 95%이상이 민간영역이라 할 때 이에 대한 정보보호는 법적근거, 전문인력, 첨단장비, 정교하고 세심한 정책과 제도수립 등이 필요함

o 정보보호 중요성이 증가함에 따라, 공공부문의 사이버위기 대응을 담당하고 있는 행정안전부, 국정원 등은 관련 조직이 지속 확대되고 있는 반면에, 민간부문의 사이버침해 위협수준이 더욱 높아지고, 피해규모가 커져가고 있음에도 불구하고, 민간부문 사이버위기 대응을 맡고 있는 방송통신위원회 정보보안 정책관련 조직은 (구) 정보통신부 시절 국 규모에서 1개 팀 수준으로 축소됨

□ 정부의 43개 중앙부처 가운데 자체 정보보호 전담부서를 운영 중인 부처는 9개에 불과함

o 자체 정보보호 전담인력은 총 78.5명으로 부처당 평균 1.45명에 불과함

*** 국무총리실(0.6명), 감사원(0.2명) 및 방송통신위원회(0.8명) 등 16개 기관이 1명 이하의 전담인력이 배치되어 있는 것으로 나타남**

*** 출처 : '7.7 DDoS 사고대응의 문제점과 재발방지 방안, 국회입법조사처(' 09.12)**

□ 국내 지식정보보안산업은 전형적인 영세 중소기업형 산업구조를 가짐

o 글로벌 기업과 경쟁하기 위해서는 M&A를 통한 산업구조의 전문화·대형화가 시급

□ 산·학·연 간 연구협력 및 융합조직 미흡

o 대학, 공공연구기관의 연구역량을 최대한 활용할 수 있도록 공공연구기간 간 협력을 전제로 한 대형 협력프로젝트 미흡

o 연구주체들의 자발적인 지식정보보안관련 아이디어 제안과 연구개발에 대한 활성화제도 미흡

3. 지식정보보안 R&D 투자 미흡

□ '07년 정부 R&D 예산 12조 2,731억원 중 지식정보보안 분야는 243억원에 불과

[그림 16] 미국과 한국의 정보보안산업 예산 비교

*** 출처 : '지식정보보안산업 진흥 종합계획', 지경부('08.12)**

□ 기업 정보보호 활동과 투자도 낮은 수준임

o 사이버 침해사고에 대응하기 위한 활동을 하지 않는다는 기업이 61.1%로, 기업의 대응역량도 미흡한 실정임

*** 7.7 DDoS 발생 당시 DDoS 보안장비를 갖추거나 여유 대역폭을 확보한 일부 기업을 제외한 대다수 기업들의 피해가 심했던 것으로 파악됨**

□ 정보화 대비 정보보호 투자 비율이 1% 미만인 기업이 '08년 66.7%에 달하여 매우 취약하고, 정보보호책임자(CSO)를 임명하고 있는 기업은 12.2%에 불과함

o 대부분의 기업이 해킹·DDoS 공격을 대응하기 위한 투자 미흡

*** 출처 : '2009년 정보보호 실태조사 ', 방송통신위원회('10.3)**

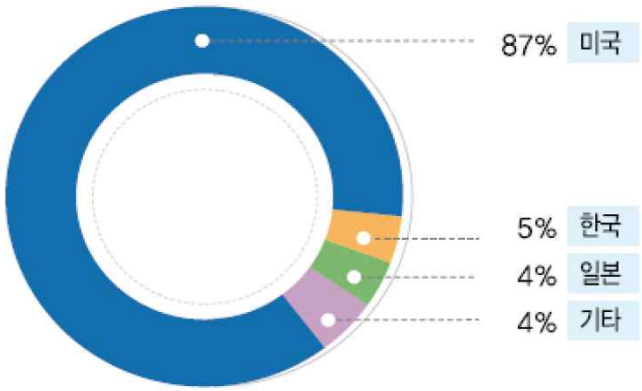
□ 지식정보보안 핵심기술의 기술력 부족

o 바이러스 백신, 안티 스팸, 기업문서용 DRM 기술은 비교적 우수하나, 네트워크 보안기술의 경우 시스코(세계2위), 주니퍼(세계7위), 시만텍 등에 비해 열세

□ 이질적인 네트워크 및 플랫폼 환경으로 인해, R&D 투자 및 기술 개발의 노력이 분석될 수 있어 네트워크·시스템 보안의 공통 기술 개발 및 표준화가 부족

□ 지식정보보안 기술수준조사 결과 비교

o 미국이 최고기술 보유국이라는 응답이 가장 많았으며(87%), 한국, 일본이 그 다음으로 소수 응답을 보임



[그림 17] 기술보유국 응답

*** 출처 : 한국산업기술평가관리원, 2009년 IT산업원천 기술수준조사**

□ 보안을 필수 기능이 아니라 선택적 부가기능으로 생각하는 잘못된 인식 및 R&D 관행 극복 필요

4. 지식정보보안 전문인력 및 인식 부족

□ 공격대응을 위한 악성코드 분석 전문인력 부족함

o 인터넷침해대응센터(KISC)의 조직, 인력이 '03년 수준에 머물러 있어 7.7 DDoS 침해사고에 보다 효과적으로 대응하기에는 한계 노출됨

o 특히, 7.7 DDoS 침해사고 당시 사고의 근원이 되는 악성코드 분석을 위한 전문인력이 3~4명에 불과함

[그림 18] 지식정보보안 분야 인력수급의 불균형

<표 6> 정부 부처별 정보보호 부서 및 인력현황

기관명	현 재		
	전담조직	정보보호인력	담당부서
합계(평균)		78.45명(평균1.45명)	
통일부	X	1	행정관리담당관
행정안전부	O	2	정보화담당관
외교통상부	O	3	외교정보보안팀
기획재정부	X	0.8	정보화담당관
노동부	X	0.75	정보화담당관
환경부	X	1.1	정보화담당관
농림수산식품부	X	0.65	정보화담당관
국토해양부	X	0.7	정보화통계담당관
문화체육관광부	X	1.5	정보화담당관
교육과학기술부	O	6	정보보호팀
법무부	X	0.8	정보화담당관
지식경제부	X	0.4	정보화담당관

보건복지가족부	X	2.75	정보화담당관
여성부	X	0.5	법무정보화담당관
국방부	O	9	정보화기획관
법제처	X	0.3	법제정보과
국가보훈처	X	1.1	정보화팀
국세청	O	6	전산정보관리과
기상청	X	1	정보통신기술과
농촌진흥청	X	1.6	지식정보화담당관실
대검찰청	X	2.5	정보통신과
문화재청	X	0.25	정보화기획팀
행정도시청	X	0.6	정보인프라과
방위사업청	X	3	전산정보관리소
병무청	X	2.3	정보기획과
산림청	X	0.7	정보통계담당관실
관세청	X	2	정보협력국
경찰청	O	10	정보통신담당관실
소방방재청	X	0.5	정보화담당관
식약청	X	0.2	정보화담당관
조달청	X	0.6	전자조달국
중소기업청	X	1.3	고객정보화담당관
통계청	O	3	통계정보국
특허청	O	2	정보기획국
해양경찰청	O	3	정보통신과
방송통신위원회	X	0.8	정보전략팀
감사원	X	0.2	지식관리담당관
국무총리실	X	0.6	인사과
민주평통	X	1	기획재정담당관
공정거래위	X	1.2	정보화담당관
금융위	X	0.3	규제개혁법무담당관
국가인원위	X	0.35	행정법무담당관
국민권익위	X	1.1	정보화담당관

*** 출처 : '7.7 DDoS 사고대응의 문제점과 재발방지 방안, 국회입법조사처(' 09.12) 행정안정부 제출자료 '09.10(직무수행률을 기준으로 산정되었으며, 국방부, 경찰청은 기관의 기관의 특성상 타 기관과 조직 규모가 매우 상이하여 평균산정에서 제외)**

□ 지식정보보안산업의 인력수급 불균형

o '07년 기준, 지식정보보안 분야 수요 인력은 31,705명이나 공급인력은 30,342명으로 인력부족 비율은 약 4.3%에 해당되며, '13년에는 인력부족비율이 약 11.8%에 이를 것으로 전망됨

*** 출처 : '7.7 DDoS 사고대응의 문제점과 재발방지 방안, 국회입법조사처(' 09.12)**

□ 사이버 위협에 대한 인터넷 이용자의 대응 미흡

o 전체 가구(16,916,966가구)의 81.4%가 컴퓨터를 보유하고 있으며, 컴퓨터를 보유한 가구당 평균 컴퓨터 보유대수는 1.38대, 개인이 보유한 컴퓨터대수는 총 19,053,635대인 것으로 추정됨

*** 출처 : '개인 인터넷 이용자 정보보호 실태조사', KISA('08.12)**

□ 컴퓨터 백신S/W 설치 및 업데이트 등 실행률이 저조하여, 전체 1,905만 여대 개인용 컴퓨터 중 15.4%(293만 여대) 이상이 악성코드 감염에 노출되어 있으며, 이는 7.7 DDoS 공격에 동원된 11만5천 여대의 약 25배에 해당됨

o 인터넷에 연결된 것으로 추정되는 PC 중 94.3%인 최소 1,295만 여대(최대 1,793만 여대)에 백신프로그램이 설치되어 있으며, 그 중 16.6%인 최소 215 만 여대(최대 298만 여대)는 월 1회 이상 바이러스 검사를 하지 않는 것으로 나타났음

<표 7> 컴퓨터 정보보호 프로그램 설치 현황

	바이러스 백신	악성코드차단 프로그램	유해정보차단 프로그램
2007년	90.0%	82.2%	51.4%
2008년	94.3%	90.6%	52.7%

*** 출처 : '개인 인터넷 이용자 정보보호 실태조사', KISA('08.12)**

<표 8> 바이러스 백신 이용방법 현황

	실시간 바이러스 감시기능 설정	바이러스 예약검사 기능 이용	월1회 이상 바이러스 검사 실시
2007년	90.0%	82.2%	51.4%
2008년	94.3%	90.6%	52.7%

*** 출처 : '개인 인터넷 이용자 정보보호 실태조사', KISA('08.12)**

o 백신 프로그램을 설치하지 않은 PC는 최소 78만 여대(최대 108만 여대)이고, 월 1회 이상 바이러스 검사를 하지 않는 PC는 최소 215만 여대(최대293만 여대)로써 293만 여대 이상이 악성코드 감염위험에 노출되어 있음

□ 정보화 역기능과 사이버위협에 대한 개인의 적극적 대응 미흡

o 이용자들은 정보보호의 중요성에는 공감하고 있으나, 정보보호 관련 최신정보를 수집하거나 대책을 마련하는 이용자는 30.2%에 불과함

o 7.7 DDoS 발생 시 보안패치에 대한 국민들의 적극적 참여부족으로 대응에 한계

* ISP가 감염 PC 이용자 8,600(1·2차 공격)명에게 무료백신 설치 안내를 하였으나 2,300명만 설치한 것으로 나타남

* 출처 : '개인 인터넷 이용자 정보보호 실태조사', KISA('08.12)

V. 지식정보보안산업 육성 방안

1. 지식정보보안산업 육성 방안

□ 정부의 규제강화 필요

o 지식정보보안분야는 국가의 수익성과 상관없이 국민 대다수에게 제공되어야 하는 공적 재화 개념이 강하고 산업차원에서도 그 중요성이 커지고 있으며, 보안이라는 특수성으로 인해, 기업 및 개인의 입장에서 볼 때에도 적극적인 정부 개입이 필요함

*** 인터넷 및 일반 분야의 산업 육성·정책·침해대응 등을 통합·일관적으로 추진할 수 있는 정부 또는 국가연구소 중심의 지식정보보안 컨트롤 타워 필요**

□ 민간 정책부서 확대 필요

o 급증하는 지식정보보안의 수요를 중앙정부 단독의 역할로서는 부족하므로 지방정부와 시민, 기업이 함께 수평적, 민주적으로 의사결정 체계를 구축하여 협력할 수 있는 민간 정책부서를 확대할 필요가 있음

□ 국가 중요정보에 대한 안전·보호를 신뢰할 수 있는 자국보안 기술과 기업이 담당토록 육성 필요

□ 보안 강화 및 시장확대를 위해서는 민간자율로는 한계가 있으며, 일정부분 정부의 규제 및 육성정책 필요

o 보안산업의 특수성으로 정부 주도 보안시스템 구축사업, 관련 법제도가 산업 성장 및 발전을 견인하도록 육성

□ 정보보안산업의 인프라 조성을 위해 산·학·연 간 연구협력 및 지식정보보안 조직 확대 필요

o 공공연구기관 간 대형 협력프로젝트 추진, 자발적 지식정보보안 조직에 대한 지원을 확대하는 등 연구개발 주제들 간의 연구·개발 협력 활성화 필요

*** 창의적인 지식정보보안산업 기술 개발에 대한 인센티브 지원 강화**

□ 시장·인력수요 확대

o IT보안 인프라가 열악한 국가 핵심기술 보유 중소기업을 대상으로

취약점 분석 등 보안 컨설팅을 실시하여 정보보안 컨설팅 시장 활성화 및 국산 정보보안 제품의 구매 유도

o 사이버테러 등 외부 침입에 따른 사회경제적 피해를 예방함과 동시에 국내 정보보안 제품 및 전문 인력의 신규 수요를 창출

□ 수출 경쟁력 제고

o 업체가 공동으로 참여하는 수출 컨소시엄 구성, 해외 로드쇼 개최 등 수출 마케팅을 지원

o 업체별 판매실적, 사이버 공격·방어 시뮬레이션 등을 소개하는 '마케팅 Reference 사이트 구축'하여 해외 홍보를 강화

o 국가기관(기술표준원)에서 인증(인정)하는 임의인증 방식의 '품질인증' 제도를 도입

- 현행 보안성 평가·인증 제도의 한계점을 극복, 국내 보안 제품의 품질 향상과 수출 경쟁력을 제고

o 지식정보보안 산업정책 지원역량을 강화하고, 보안산업 전체를 아우르는 입체적인 지원체제를 구축

2. 지식정보보안산업 기술 R&D 확대

□ 국가보안의 특수성을 고려하여 제도적 측면에서 국가적 R&D 프로그램 발굴 추진

o 핵심 지식정보보안기술의 경우 국가안보와 직결되는 사안인 만큼 단순 경제적 논리로 접근하지 말고 안보차원에서 과감한 R&D 투자 필요

o 사이버 보안과 관련된 R&D 프로그램 개발법을 지정하여 국가 차원에서 사이버보안 관련 연구프로그램 기술 확보

□ 국가 R&D 결과물의 활용도 및 상용화 성공률 제고를 위한 수요자 연계 강화

o 사업자, 산업체, 기업 등 수요자의 공동연구 참여를 유도하여, 사업 초기단계부터 시장에서 필요한 요구를 반영할 수 있도록 조기 상용화 전략 및 핵심 기술 개발 병행 추진

o 중장기적으로 민간이 수행하기 어려운 지식정보보안 핵심 공통 기술의 조기 개발을 통한 미래 원천 기술 확보 후, 서비스·인프라 구축 단계에서 시범적용 및 검증 강화를 실용성 있는 기술 확보에 주력

□ 국내 지식정보보안분야 기술의 국내외 경쟁력 강화 및 표준화 선도를 위한 우수 기술의 국제 표준화 중점 영역 발굴 추진

o TTA, IETF, ITU-T 등 국내·외 기술표준화 환경 분석, 기술·상용화 성숙도 수준 분석 등을 통한 선택과 집중이 필요한 중점 표준화 영역 발굴

o SEED 등 국산 암호·인증기술들이 의료, 국방 등 다양한 산업 분야에 활용 될 수 있도록 표준화 추진 영역을 선행 발굴하여 국제 표준화 선도 가능 분야 육성

o 봇넷 대응 체계, 스팸 대응 등 국내 기술의 강점 분야의 미국, 유럽 등 주요국과의 전략적인 해외 국제 표준화 공동 제휴·협력 강화

□ 타 산업 분야 연계 강화를 통한 신규 융합 보안 시장 창출

o 지식정보보안기술은 ICT 인프라를 이용한 타 산업기술의 핵심 필수 요소 기술로서, 기술·산업간 급격한 융합화 트렌드에 따라 신속한 대응을 위한 타 산업 분야 기술 연계 확대 필요

* ICT : Information & Communication Technology(정보통신기술)

o 기존의 지식정보보안 핵심기술을 활용하고, 타 산업 분야에 활용 가능하도록 공통 플랫폼화 및 커스터마이징 강화를 통한 타 산업 응용 보안 기술 확보

□ 원천핵심기술 개발을 위한 R&D 예산 확대

o 전략산업 경쟁력 제고를 위해 핵심 SW 기술 개발을 위한 예산 확대

o 사이버보안 관련 기관이 적극적으로 활동할 수 있도록 관련 예산을 적절히 반영할 수 있는 근거 마련

□ R&D 결과물의 해외 추출지원 및 홍보활동 강화

o 기술력이 우수한 중소기업 보안 제품의 패키지 수출 지원

o 해외 전시회 및 업체 홍보책자 발간 등 해외 홍보 지원 강화

3. 지식정보보안산업 교육 투자 확대

□ 지식정보보안산업 인력의 경쟁력 강화 및 지식정보보안산업에 적합한 시장중심 인재 양성

o 지식정보보안 기술을 토대로 한 디지털 포렌식, 융합보안 등의 분야에 대한 고급인력 양성 추진

o 대학 IT 연구센터 육성, 지원 사업으로 융합보안 고급인력 양성

□ 시장중심 지식정보보안 인재 양성

o 산학연계를 통한 실무적합 인력 공급
- 기업과 대학이 공동으로 교과과정을 개발하고 졸업생을 채용하는 고용계약형 석사과정 도입

o 공개 SW인력 양성
- 대학내 공개 SW기반의 개발자 커뮤니티 설립 지원

o 재교육을 통한 지식정보보안산업 인력 업그레이드
- 기업 재직자를 대상, 수준별 기업수요 맞춤형 지식정보보안 인력 양성사업 추진

o 지식정보보안산업 기반 학제연계 교육과정 신설
- 자동차, 항공, 조선 등 도메인 지식과 지식정보보안산업 및 소프트웨어공학교육의 융합을 지원하는 융합기술 교육

□ 지식정보보안산업 인력의 글로벌 경쟁력 강화

o 지식정보보안산업 교육의 질적 수준 제고
- 현행 응용 소프트웨어활용 위주에서 문제해결 역량을 중심으로 초중고 교과과정 개편

o 대학의 신규 지식정보보안 인력 역량강화
- 글로벌 지식정보보안 인재 양성을 위한 교육과정 설치 지원
- 잠재력이 있는 우수학생들을 선발하여 학·석사 통합과정을 통해 선발하여 교육과정 지원

□ 대국민 보안인식 제고

o 사이버 공간 보호를 위한 국가전략으로 모든 국민에게 자신의 사이버 공간을 보호할 수 있는 능력을 부여하는 국가 인식 프로그램 운영

o 개인정보보호에 대한 중요성 인식 제고를 위한 민간 부문 지원 확대

o 일반 국민을 대상으로 하는 지식정보보안 기초 교육전담 기관 및 교육과정 신설 필요