BM 개발 및 수요발굴을 통한 대형기술마케팅 : BM-SMK

ETRI 한국전자통신연구원

지능형 사이버 공격 인지 및 추적기술

(주)델타텍코리아
기술사업화 자문회사

Summary

Lab 현황	• 세계 IT보안 트렌드가 사이버 보안 위협 대응 측면에서는 "산업적 문제"에서 "국가 안보적 문제"로, 보안 기술 및 시스템 측면에서는 "다기능/속도 경쟁"에서 "소프트웨어 지능 경쟁"으로 변화되고 확대되는 추세에 따라 다양한 정보보호 영역에 대한 연구/개발을 중점 추진하고 있음
기술 개요	• 주요 IT기반 시설의 정보시스템의 안정성을 보장하기 위한 호스트, 네트워크 등 다중 소스 데이터의 Long-term history 분석기반 사이버 표적공격 인지 및 공격자 추적 기술
기술 동향	• **(지능형보안기술)** 표적공격 방어를 위해 네트워크 및 시스템 보안 제품군을 통합한 보안 이벤트 정보 관리기술을 제공하고 있으며, 이를 바탕으로 빅데이터 처리기술을 활용한 지능형 보안 기술에 대한 연구가 본격화 되고 있음 • **(네트워크기반 악성코드 추적)** 네트워크 기반의 추적은 제한적으로 연구가 진행되고 있으며 상용 제품으로 출시가 이루어지지 못하고 있음
시장 동향	• 국내 정보/물리보안산업 매출액은 2010년 4조 40억 원 에서 2013년에는 7조 1,454억 원으로, 연 평균 15.2%의 높은 성장률을 보임 • 국내 정보/물리보안산업 수출액은 2013년 기준 1조 5,487억 원으로, 연 평균 28.7%로 성장하고 있음 • 국내 정보보호 시장은 세계시장의 2.8에 불과하지만, 이에 반해 국내 IT 시장 규모는 세계 IT 시장의 약 10% 내외 수준 • 미국의 경우 세계 정보/물리 산업의 40%를 차지하고 있으며, 연평균 10%대의 높은 성장세를 나타냄 • 미국은 사회기반시설 사이버보안 프레임워크 마련을 본격화하고 있으며, 백악관 직속 사이버 사령부 창설, 국가사이버보안종합계획 등 중장기 전략 수립 추진 등 정보보호 R&D 비중 강화를 통한 꾸준한 투자를 하고 있음
협력 사업	• ㈜인포섹, ㈜SK-C&C 통합 보안관제 센터에 빅데이터 분석 공격인지 시스템 프로토타입을 설치 운영하여 시스템 검증 중 • KT Kornet 및 국가망 연동 역추적 테스트베드 구축 • '한예종-기관 사이버 안전센터-국가 사이버안전센터' 연동 통합 시험 사업 구축

목차

ETRI 사이버보안시스템연구부(네트워크보안연구실)

VISION : 다양한 정보보호 영역에 대한 연구/ 개발을 중점 추진

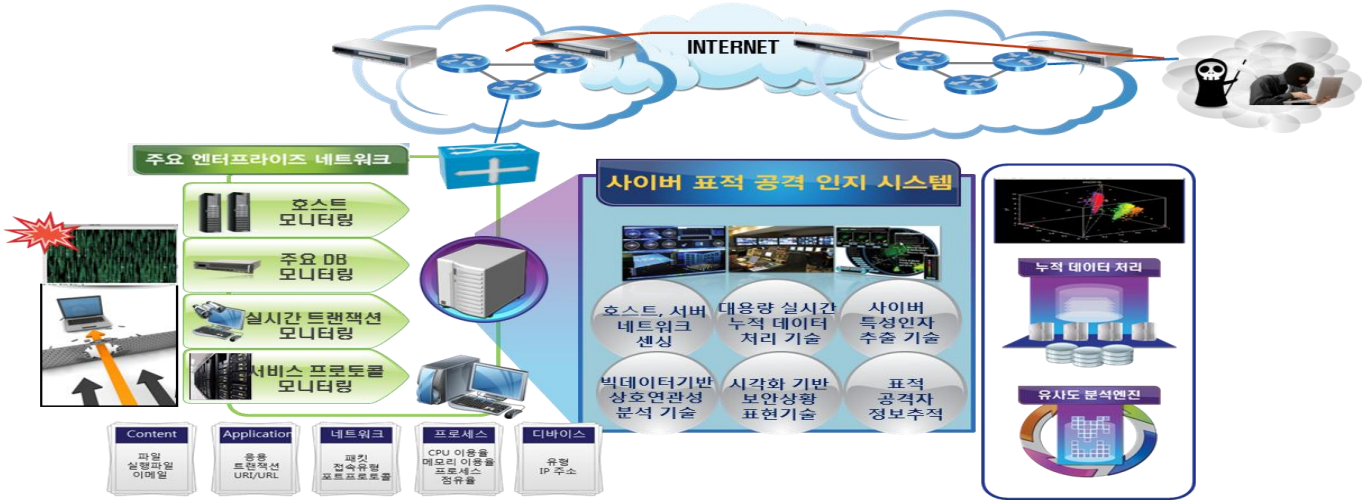
목표

무범죄 안전 국가 건설을 위한 국가사회의 현안 문제 해결 및
산업 경쟁력을 제고하는 R&SD 역량 확보

- 실시간 분석을 위한 디지털 포렌식 기술 연구
- 데이터 프라이버시 보호 기술 연구
- 스마트지갑 2.0 기술 연구
- 디바이스 보안 분석 연구 / 융합 보안 연구
- 영상보안 연구 / 가상화 기반 스마트 단말 보안기술 연구
- 대용량 데이터 분석기반 사이버 표적공격 인지 및 추적기술 연구
- 스마트 단말의 정보유출 방지를 위한 MTM기반 보안 핵심 기술 연구

□ 기술의 간략한 소개

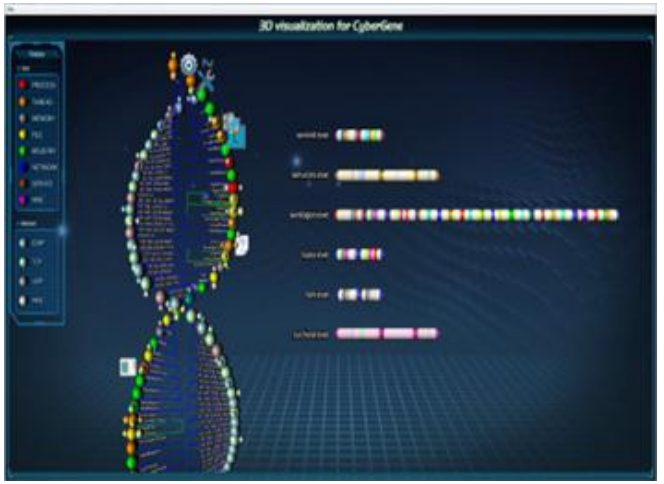
- 주요 IT기반 시설의 정보시스템의 안정성을 보장하기 위한 호스트, 네트워크 등 다중 소스 데이터의 Long-term history 분석기반 사이버 표적공격 인지 및 공격자 추적 기술
- 어플리케이션 사이버 게놈(SINBAPT-Gene), 공격자 근원지 정보 추적(SINBAPT-Tracker), Signaure-less AV엔진(SINVATP-SigFree AV) 등 세 가지의 세부기술로 개발됨



<지능형 사이버 공격인지 및 추적 개요도>

□ 어플리케이션 사이버 게놈(SINBAPT-Gene)

- Host/Network 특성인자 DNA 정보를 추출하여 모델링하고, 어플리케이션 실행 파일에 대한 행위 패턴 분석 결과를 3D 시각화 엔진을 통해 표현하여, 사이버 표적공격 징후에 대한 직관적 분석 기능을 제공



< Host/Network 특성인자 DNA 정보 추출 개요 >

□ 어플리케이션 사이버 게놈(SINBAPT-Gene)

○ 기술 구현 방법

① 사이버 표적공격 특성인자 DNA 정보 제공

② Host/Network 분석 모델 상세 정보 제공

③ 3D 시각화 엔진 기반 직관적 분석

④ 어플리케이션 실행 파일 행위 패턴 스캔 및 상세 정보 제공

⑤ 어플리케이션/악성코드 군(群) 별 3D 이미지화

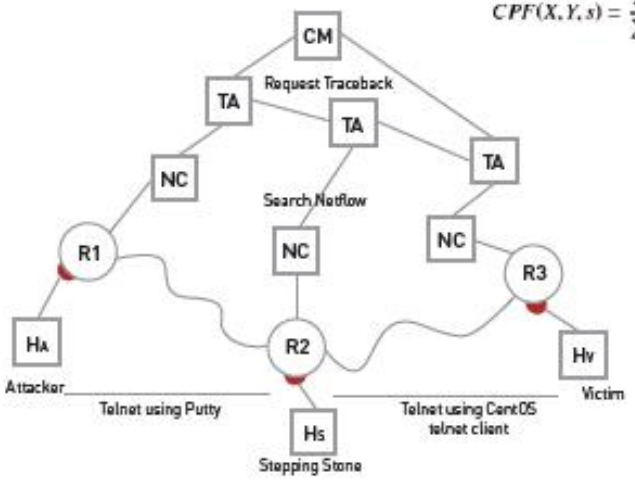
○ 시스템 사양

운영체제	CPU	Memory	요구 플랫폼	Languages
Windows 7 (64bit/32bit)	Intel Core i5 Over	16GB over	Oracle 11g / MySQL	Java/Graphics 2D/ OpenGL/ MonkeyEngine3

□ 공격자 근원지 정보 추적(SINBAPT-Tracker)

- Router로 부터 수신되는 Netflow 기반의 Connection 정보들을 분석하여 관련 Connection에 대한 Finger Print 정보를 생성하여 공격 근원지의 실시간 추적

$$CPF(X,Y,s) = \frac{\sum_{j=1}^{m} min(x_j, y_{j+s})}{\sum_{j=1}^{m} max(x_j, y_{j+s})}$$



< 사이버 공격 근원지 추적 개요>

□ 공격자 근원지 정보 추적(SINBAPT-Tracker)

○ 기술 구현 방법

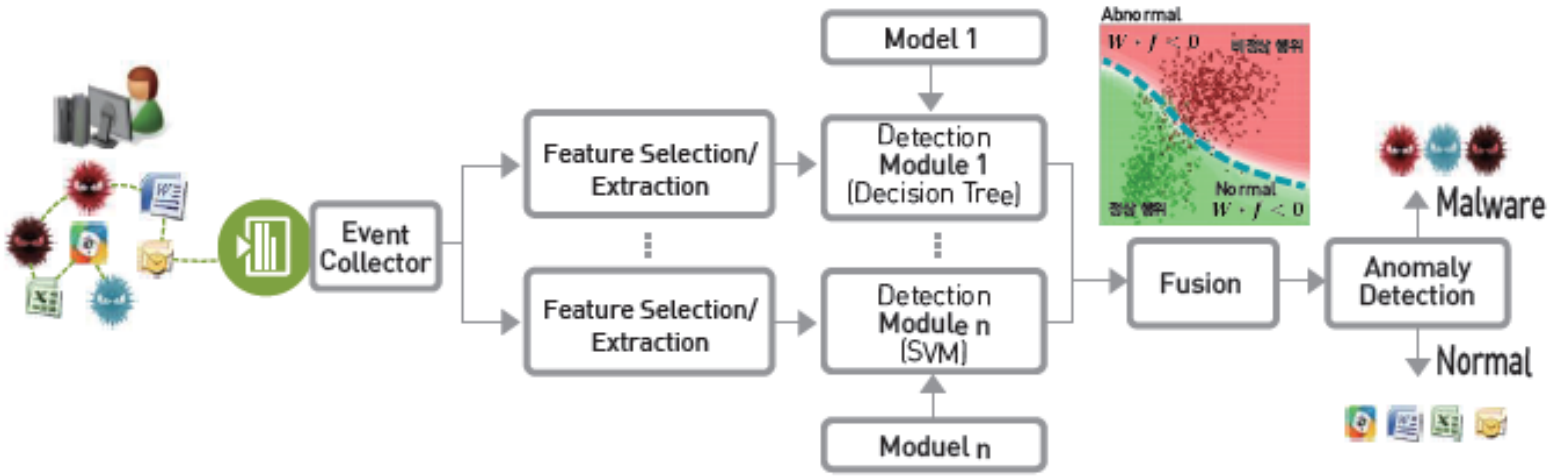
- Netflow Collector : Router로 부터 Netflow v5 정보 수집 및 저장
- Central P2P Manager : P2P 기반 Netflow 정보 수집 및 공유
- Traceback Agent : NetFlow 정보 기반 역추적 분석
- Correlation Point Function : Finger Print Algorithm을 통한 Flow 검색
- 3D GUI : 위성 GPS 기반의 3차원 사용자 인터페이스 제공
- 공격근원지, 경유지, 공격피해지 분포 및 연결상태 분석

○ 시스템 사양

운영체제	CPU	Memory	요구 플랫폼	Languages
NFTB-CentOS	Intel Core i5 Over	16GB over	GCC4.4/JDK1.6/ MySQL5.5	C/Java
3D GUI-Windows 7	Intel Core i5 Over	8GB over	Spring 3.1/MyBatis 3.1/JDOM 1.1	Java, JavaScript/ HTML5/CSS3

☐ Signaure-less AV엔진(SINVATP-SigFree AV)

- 호스트에서 발생하는 다양한 행위 이벤트에 대해 데이터 마이닝 기반 빅데이터 분석을 통한 악성코드 분석/탐지 엔진



< 데이터 마이닝 기반 빅데이터 분석 개요>

□ Signaure-less AV엔진(SINVATP-SigFree AV)

○ 기술 구현 방법

① Zero-day 악성코드 탐지를 위한 Signature-less 호스트 이상행위 탐지

② 47종 이상의 호스트 행위 이벤트에 대한 커널 레벨 실시간 수집

③ BigData 처리를 위해 데이터 마이닝 기반 악성/정상 행위 모델 생성

④ 악성코드 동적 분석을 위한 Virtual Machine 기반 비정상행위 탐지

⑤ 악의적인 프로세스 강제종료 방지를 위한 프로그램 자체 보호

○ 시스템 사양

운영체제	CPU	Memory	특징
Windows 7 (추후확장)	Intel Core i5 Over	32GB over	Virtual Machine 환경 동작 가능
			호스트 행위 이벤트 선택적 수집 가능
			호스트 프로세스 선택적 데이터 수집 가능

□ 기존 기술대비 우위성

- 특징

- Zero-day 악성코드 탐지를 위한 Signature-less호스트 이상 행위 탐지 엔진개발 (SINBAPT-SigFree AV)
- 사이버게놈 분석기반 알고리즘 개발(SINBAPT-Gene): 표적공격 특성인자 DNA 모델링
- 해킹 경유지/공격지 역추적 알고리즘 세계최초 개발(통신 3사(KT, SKBB, LGU+) 및 해외사이트 연동 시험 완료 - xFlow 정보기반 역추적 알고리즘 (세계 최초 해킹 공격자 경유지, 근원지 추적 알고리즘)

- 장점

- 마이닝 기반 이상행위 동적 분석 알고리즘 확보(Zero-day 악성코드 진단율 국내 최고 알고리즘)
- 호스트 행위기반 악성코드 탐지 엔진 시험결과 세계 최고 수준 : 탐지율(96.9%), 오탐율(4.6%)

□ 경쟁 우위

- **본 기술은 사이버 표적 공격(APT)과 같은 알려지지 않은 치명적 공격 대응에 우수한 차세대 보안정보 분석 기술로 평가 받고 있으며, 기술/ 경제/ 사회적으로 경쟁 기술 대비 파급효과가 클 것으로 기대됨**

※ 파급효과

기술	- (응용 및 확장성) 호스트PC에서 발생하는 **행위이벤트 데이터 분석을 위한 데이터마이닝 기술 확보는 보안로그 빅데이터를 분석하는 SIEM 시장으로 사업영역 확대** 예상 - 컴퓨터 바이러스 백신분야 세계 선도기업과 차별화된 기술력으로 경쟁력 확보 및 기술 의존도 감소 - 지능화, 고도화되는 보안 위협에 대응하는 **지능형 보안 시스템 구축을 위한 빅데이터 활용분야**의 하나로 사이버 보안기술의 고도화 기술로 활용
경제	- SIEM시장은 **로그관리 외에도 통합모니터링/접속관리 등으로의 활용 영역 확대**로 보안플랫폼 개발(보안/운용/어플리케이션 분석)을 통한 **통합보안관제 분야 활용 가능** - 공격자 경유지/근원지 추적 핵심기술 기반 역추적을 위한 서비스 및 비즈니스 모델 창출 - 데이터 마이닝 기반의 알려지지 않은 신종/변종 악성코드 탐지 기술 확보로 세계시장 점유율 향상 기대(국내 기업의 세계시장 점유율은 2% 이하)
사회	- 네트워크 안정성 확보로 국가적 이슈인 사이버 표적 공격에 대응하여 경제적, 사회적 피해 최소화 - 사용자/기업이 안심하고 서비스를 이용/제공하는 인터넷 망 환경조성과 사이버 공격에 따른 국가 인터넷 서비스 장애에 대한 불안감 해소

□ 목표제품/서비스

분야	보안 관제 시스템

제품	기능
• 방화벽 • 라우터 • 백신프로그램 (휴대단말기, 개인 / 회사 컴퓨터 등) • 네트워크 인증(메시지 보안, 사용자 인증)	• 지능형 사이버 공격 인지 • 해킹 경유지 및 공격지 역추적 가능 • Zero-Day 악성코드 진단율 : 96.9%

서비스

백신 프로그램

휴대단말기

개인 / 회사 컴퓨터

방화벽 및 라우터

방화벽 서비스

라우터

□ 기술완성도(TRL 단계)

- 본 기술은 Pilot단계 시작품 신뢰성 평가가 진행중인 TRL 7단계

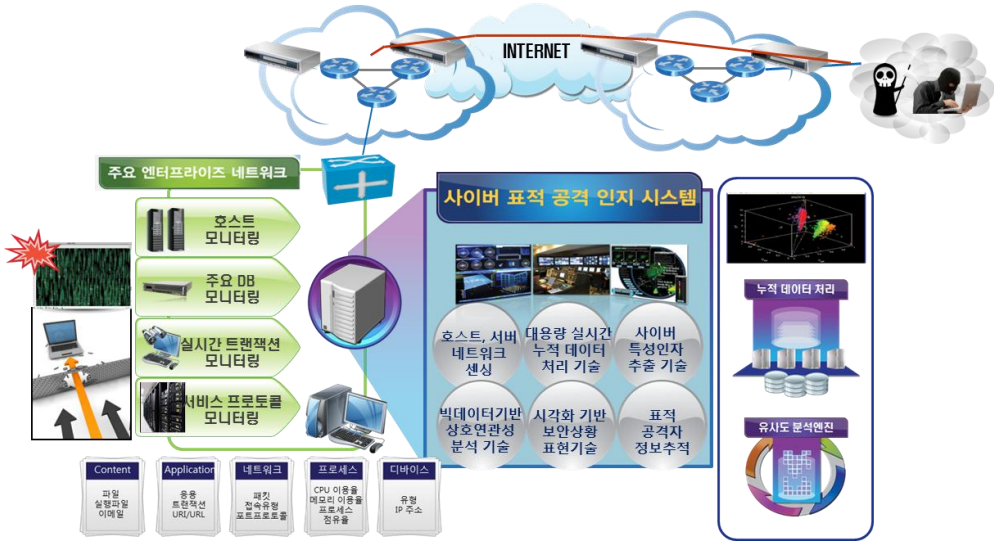
TRL 9	사업화	▪ 본격적인 양산 및 사업화 단계
TRL 8	시작품 인증/ 표준화	▪ 일부 시제품의 인증 및 인허가 취득 단계 - 조선 기자재의 경우 선급기관 인증, 의약품의 경우 식약청의 품목 허가 등
TRL 7	Pilot 단계 시작품 신뢰성 평가	▪ 시작품의 신뢰성 평가 ▪ 실제 환경(수요기업)에서 성능 검증이 이루어지는 단계
TRL 6	Pilot 단계 시작품 성능 평가	▪ 경제성(생산성)을 고려한, 파일로트 규모의 시작품 제작 및 평가 ▪ 시작품 성능평가
TRL 5	시제품 제작/ 성능평가	▪ 개발한 부품/시스템의 시작품(Prototype) 제작 및 성능 평가 ▪ 경제성(생산성)을 고려하지 않고, 우수한 시작품을 1개~수개 미만으로 개발
TRL 4	연구실 규모의 부품/시스템 성능평가	▪ 연구실 규모의 부품/시스템 성능 평가가 완료된 단계 ▪ 실용화를 위한 핵심요소기술 확보
TRL 3	연구실 규모의 성능 검증	▪ 연구실/실험실 규모의 환경에서 기본 성능이 검증될 수 있는 단계 ▪ 개발하려는 시스템/부품의 기본 설계도면을 확보하는 단계 ▪ 모델링 / 설계기술 확보
TRL 2	실용 목적의 아이디어/특허 등 개념 정립	▪ 실용 목적의 아이디어, 특허 등 개념 정립
TRL 1	기초 이론/실험	▪ 연구과제 탐색 및 기회 발굴 단계

□ 지식재산권 현황

연번	기술구분	특허종류	특허번호	제목
1	SINBAPT Sigfree AV (공격자 탐지 기술)	출원	10-2015-0020977	명령어 집합의 행위 패턴을 엔-그램 방식으로 모델링하는 방법
2		출원	10-2015-0017334	새로운 공격 유형의 자동 탐지 및 공격 유형 모델 갱신을 통한 지능형 침입 탐지 시스템 및 방법
3		등록	14/603241(미국)	APPARATUS AND METHOD FOR DETECTING A MALICIOUS CODE BASED ON COLLECTING EVENT INFORMATION
4		출원	10-2014-0012280	악성코드 분석을 위한 수집 데이터 표현 방법
5	SINBAPT – Tracker (공격자 추적시스템)	출원	출원 중	Netflow 기반 Connection FingerPrint 생성 및 공격자 역추적 방법
6		등록	14/249811(미국)	The system and method for real-time malware detection based on web browser plug-in
7		출원	10-2013-0163612	Web 브라우저 플러그인 기반 실시간 악성코드 탐지 및 보안 시스템
8	SINBAPT – Gene (악성코드 분류기)	출원	10-2015-0020976	악성코드를 탐지하기 위한 전자 시스템 및 방법
9		출원	10-2014-0003781	이상행위 탐지 및 방법
10		등록	14/596188(미국)	APPARATUS FOR ANALYZING THE ATTACK FEATURE DNA AND METHOD THEREOF
11		출원	10-2014-0012271	공격 특성 DNA 분석 장치 및 그 방법

□ 응용분야(SFN 분석)

- Seed
  - Zero-day 악성코드 탐지를 위한 Signature-less 호스트 이상행위 탐지 엔진
  - 사이버게놈 분석기반 알고리즘 / 해킹 경유지/공격지 역추적 알고리즘
- Function
  - 사이버 특성인자 모델링 / 특성인자 프로파일링 및 실시간 분석
  - 사이버 특성인자 Long-term기반 연관성분석 / 빅데이터 플랫폼기반 대용량 분산 데이터처리
  - 넷플로우 정보 분석기반 공격자 연결체인 정보 분석
- Need
  - 지능형 사이버 표적공격 선제적 대응 시스템



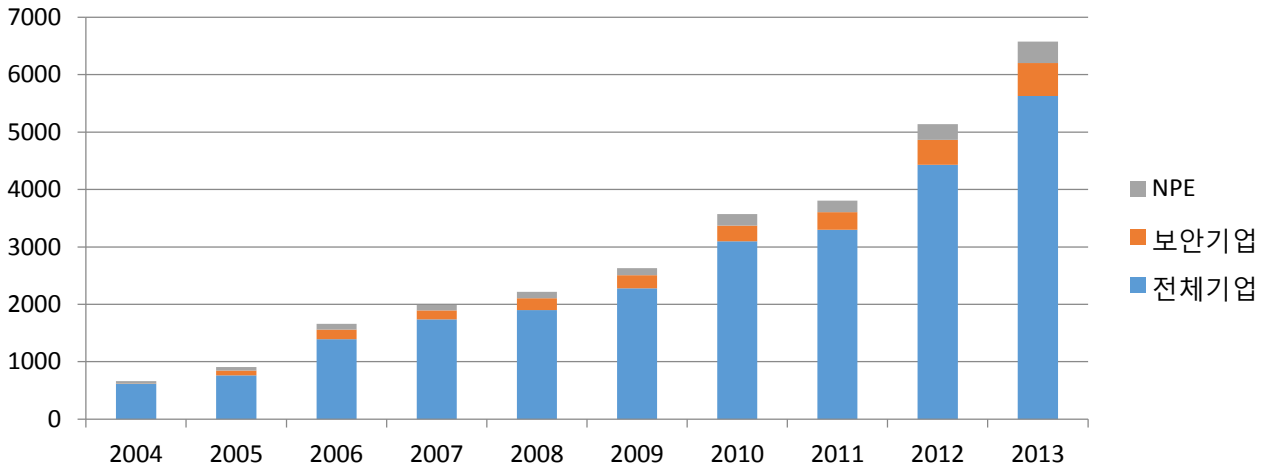
< 지능형 사이버 공격인지 및 추적 개요도>

□ 목표시장

- 본 기술의 목표시장으로 라우터, 방화벽 산업(1차)과 백신 프로그램 및 네트워크 인증 산업(2차)으로 아래와 같이 나눌 수 있음

□ 국내 특허 출원 동향

- 지식정보보안산업의 전체 특허 동향을 살펴보면, 2014년까지 평균 32% 증가하는 추세를 보이고 있음
- 지식정보보안 기업의 특허 등록도 평균 36%정도 꾸준하게 증가 하고 있으나 정보보안 기업의 특허 등록량은 전체 특허의 12%정도로 정보보안 기업의 특허 등록 점유율은 미미한 실정임
- NPE에 의한 등록 특허는 평균 26%로 꾸준하게 증가하고 있으며, 특히, '11~'13년 사이에 NPE에 의한 등록특허수가 가장 많음



* 출처 : 글로벌 지식정보보안산업 특허 동향 조사 연구(KISA, 2014)

□ 국내 특허 출원 동향

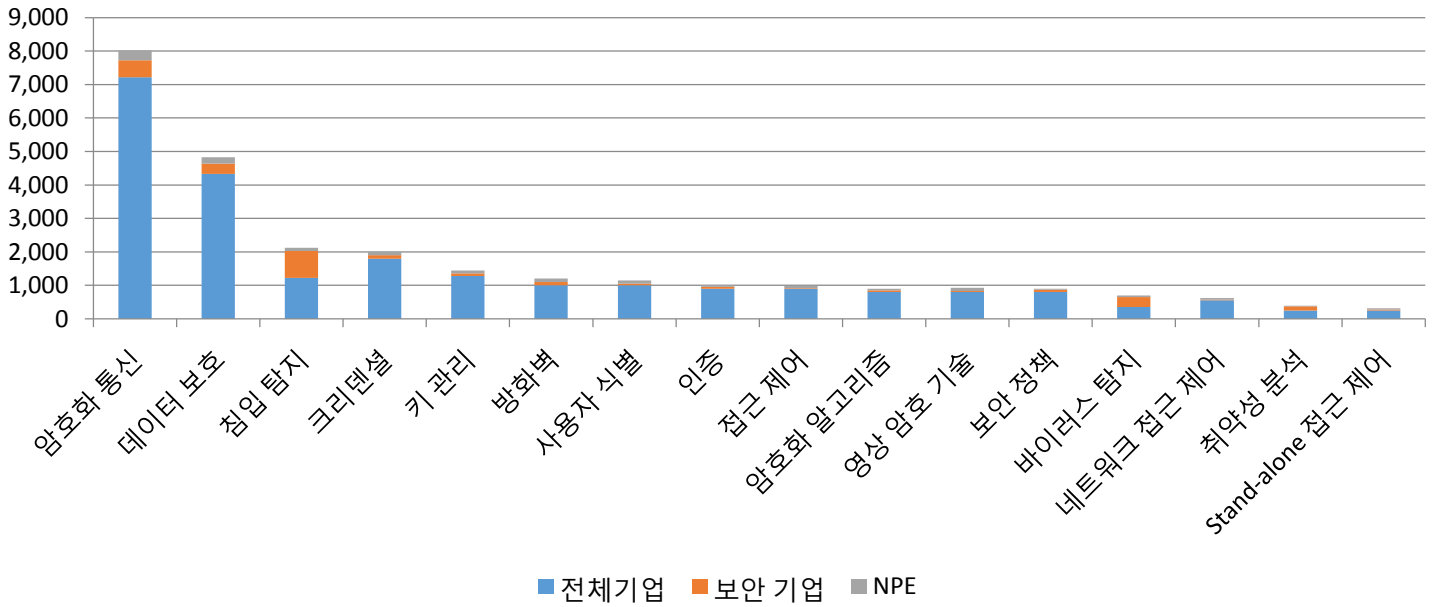
- 지식정보보안기술 보유 기업 중 가장 많은 등록특허를 보유하고 있는 기업은 MICOSOFT, INTERNATIONAL BUSINESS MACHINES, CISCO TECHNOLOGY, INTEL 등 글로벌 대기업들이며, 정보보안 특허 보유는 하드웨어 기업보다 소프트웨어 기업에 집중되어 있음
- 보안 기업으로는 SYMANTEC이 가장 많은 등록 특허를 보유하고 있어, 지식정보 보안 기술을 보유한 전체기업 중 5위를 차지하고 있음
- AT&T INTELLECTUAL PROPERTY, VERIZON PATENT & LICENSING, INTEL LECTUAL VENTURES, THOMSON LICENSING 등 특허관리전문회사 및 NPE의 보안 특허 보유도 다수 나타나고 있음

권리자	Microsoft	INTER NATIONAL BUSINESS MACHINES	INTEL	CISCO TECHNOLOGY	HEWLETT-PACKARD DEVELOPMENT COMPANY	SYMANTEC	SONY	SAMSUNG ELECTRONICS	MCAFEE	ORACLE INTER NATIONAL
등록특허	2,053	1,895	812	775	667	652	633	489	459	361
공개특허	3,128	3,537	1,347	1,003	1,152	738	972	1,135	649	485

* 출처 : 글로벌 지식정보보안산업 특허 동향 조사 연구(KISA, 2014)

□ 국내 특허 출원 동향

- 지식정보보안산업의 기술 분야 중 가장 많은 등록 특허가 포진하고 있는 기술 분야는 암호화 통신 분야, 데이터 보호 그리고 침입 탐지 기술 순으로 나타남
- 보안 기업이 다수 보유한 특허는 암호화 통신, 침입 탐지, 바이러스 탐지 기술 분야이며 NPE가 다수 보유한 특허는 암호화 통신, 데이터 보호로 권리자의 특성에 따라 보유하고 있는 기술 분야의 점유가 다르게 나타나고 있음



* 출처 : 글로벌 지식정보보안산업 특허 동향 조사 연구(KISA, 2014)

□ 주요국 시장동향

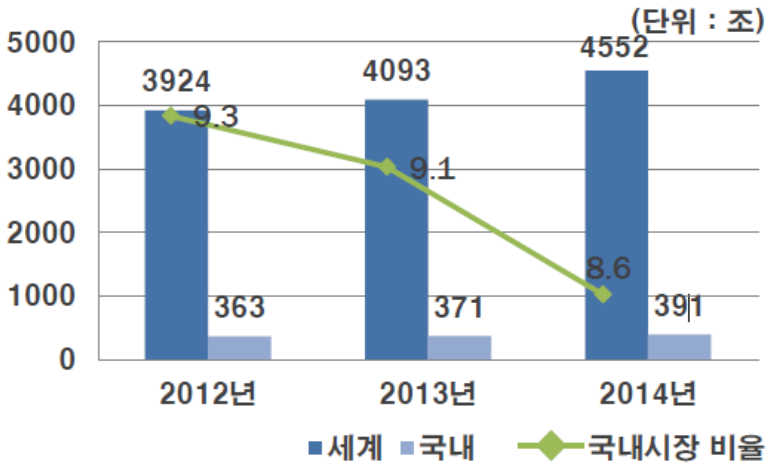
- IT산업과 정보보호산업 시장 비교

- 국내 정보보호 시장은 세계시장의 2.8%에 불과함(2013년 기준)

  * 이에 반해 국내 IT시장 규모는 세계 IT 시장의 약 10% 내외 수준

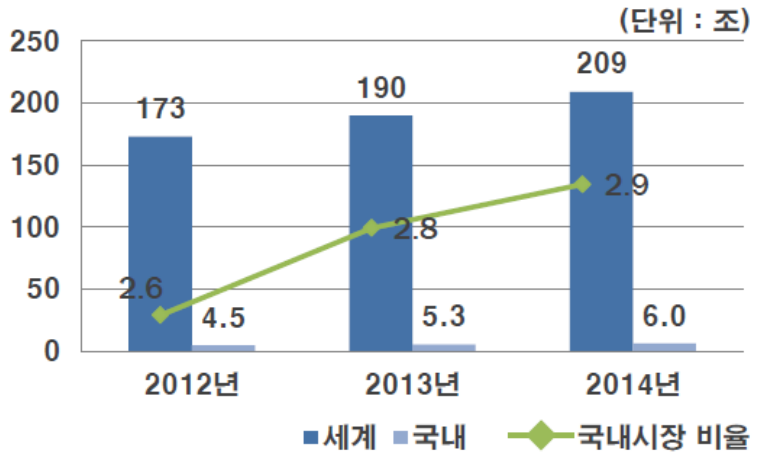
- 국내 IT산업 시장 중 정보보호산업이 차지하는 비율은 약 1.3%

  * 세계IT산업 대비 정보보호산업이 차지하는 비중은 약 5% 수준



* 출처: 2014년 ICT 시장 전망(정보통신정책연구원)

< 세계IT 시장 대비 국내 IT산업 시장 규모>



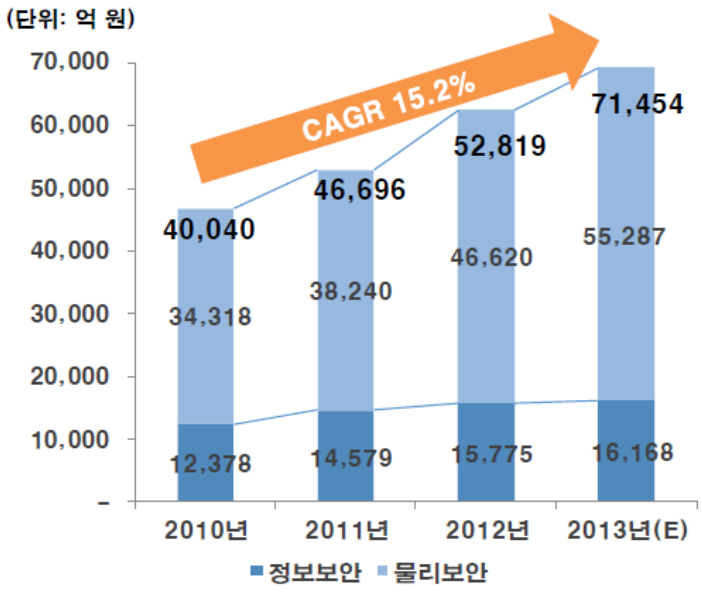
*출처: 2013 국내 정보보호산업 실태조사(KISIA・KDCA)

< 세계 정보보호시장 대비 국내 현황 및 전망>

□ 주요국 시장동향

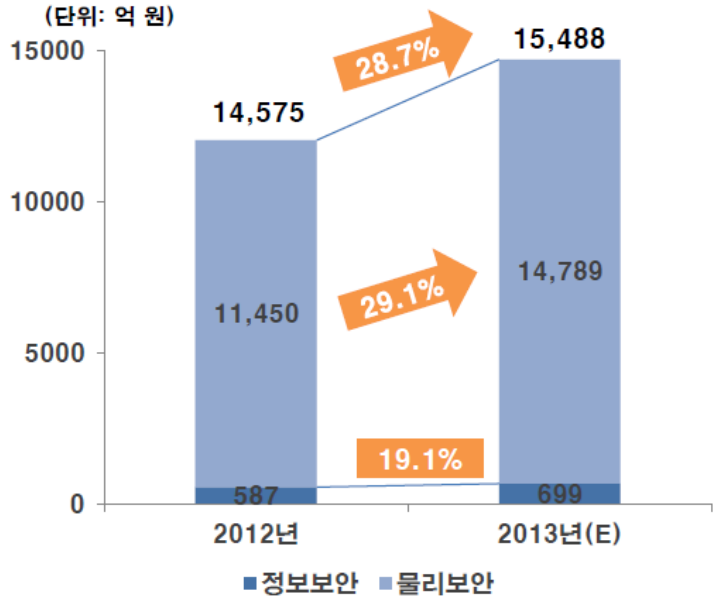
▪ 국내 시장동향

- 국내 정보·물리보안산업 매출액은 7조 1,454억 원으로 전년 대비 35.2% 증가('13년) / 수출액은 1조 5,487억 원으로 전년 대비 28.7% 증가('13년)



* 출처: 정보보호산업 전망(한국인터넷진흥원, 2014)

< 정보보호산업 매출 규모>



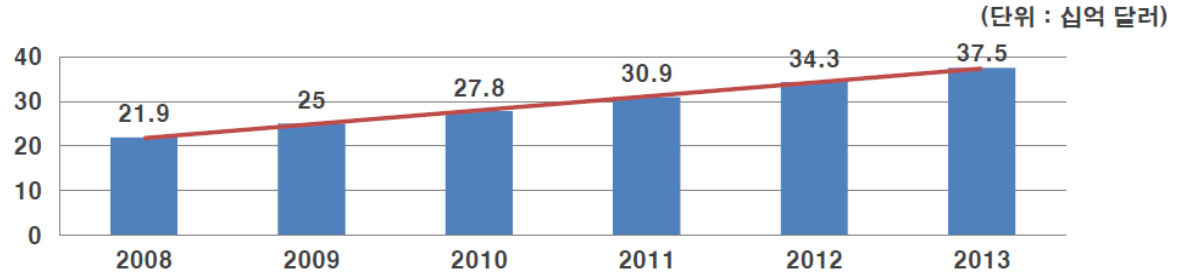
* 출처: 정보보호산업 전망(한국인터넷진흥원, 2014)

< 정보보호산업 수출 규모>

□ 주요국 시장동향

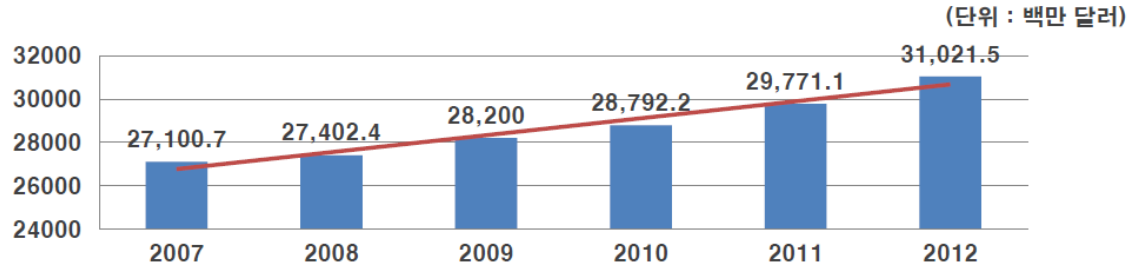
▪ 글로벌 시장동향

- (정보보안 분야) 세계 시장의 약 40%를 차지하고 있으며, 연평균 10%대의 높은 성장세를 보임
- (물리보안 분야) 2012년 건설 및 주택 경기의 활성화와 교체 수요에 힘입어 4.2%의 높은 증가세를 보임



* 출처: 글로벌 정보보호산업 동향조사(한국인터넷진흥원, 2013)

< 정보보안 분야 시장규모>



* 출처: 글로벌 정보보호산업 동향조사(한국인터넷진흥원, 2013)

< 물리보안 분야 시장규모>

□ 주요국 시장동향

▪ 글로벌 시장동향_미국

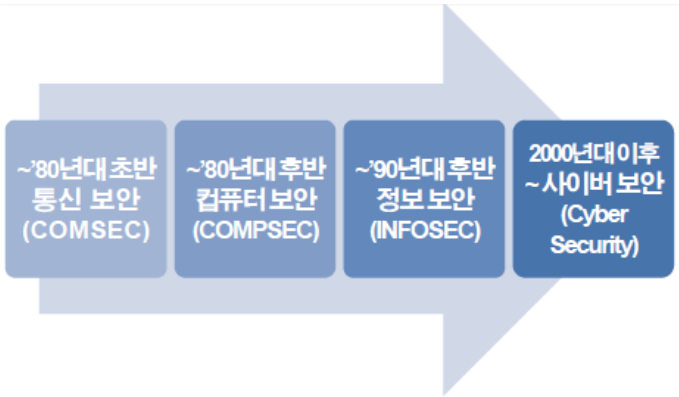
- 사회기반시설 사이버보안 프레임워크 마련 본격화

- 오바마 대통령은 주요 사회기반시설에 대한 사이버 위협에 대처하기 위해 행정 명령 1 (Executive order)을 지시('13.2.12)

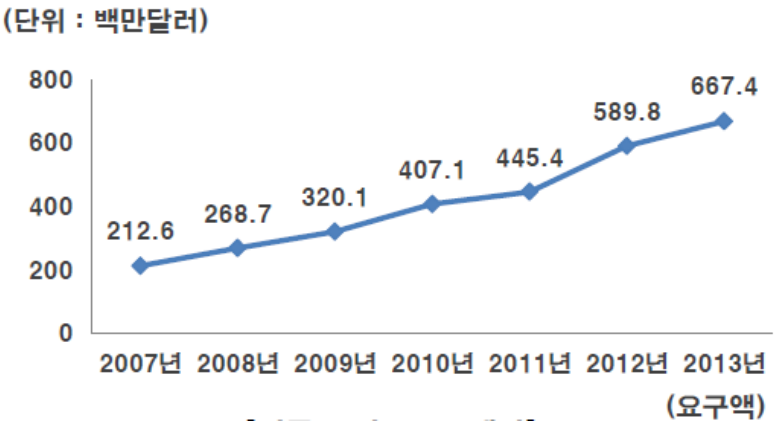
  * 미국 내 사회기반시설을 운영하는 기업들이 사이버 보안기준 프로그램을 마련하도록 하는 것을 주요 골자로 하고 있음

- 백악관 직속 사이버 사령부 창설, 국가사이버보안종합계획 등 중장기 전략 수립 추진
- 정보보호 R&D 비중 강화를 통한 꾸준한 투자

  * '11년 대비 정보보호 R&D 예산 50% 증가



< 단계별 미국의 보안정책 추진>



< 미국 보안 R&D 예산>

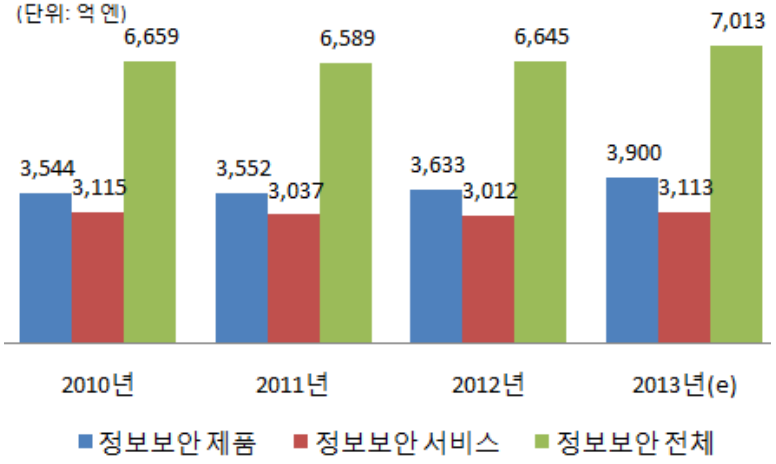
* 출처: 글로벌 정보보호산업 동향조사(한국인터넷진흥원, 2013)

□ 주요국 시장동향

- 글로벌 시장동향_일본

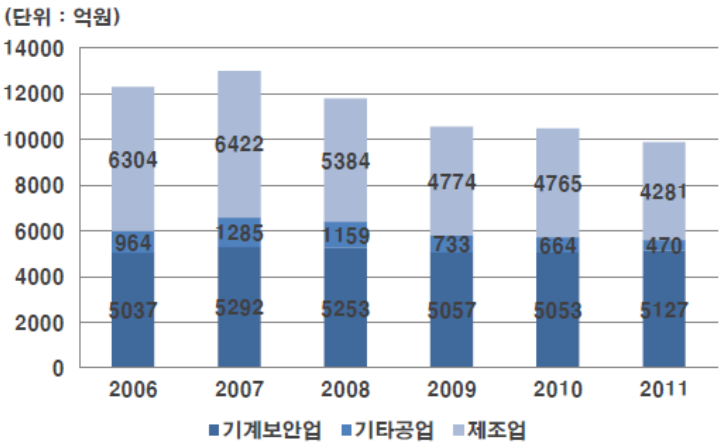
- (정보보안 분야) 2008년 정점에 오른 후 글로벌 경기 침체와 함께 2009년 하강 국면에 들어섰으나, 2012년부터 다시 성장세에 돌입해 2013년 약 7,000억 엔 규모에 이를 전망

- (물리보안 분야) 최근 가정 및 기업에서 수요가 증대하고 있으나, 업체 간 경쟁 심화, 기업의 비용 절감·투자 억제 등으로 가격 인하 압박이 심함



* 출처: 일본 정보보안 시장규모 및 전망, JNSA, 2013

< 일본 정보보안 시장규모 >



* 출처: 일본 기계(물리)보안 시장 규모 추이 전망, 공익사단법인 일본방범설비협회, 2013

< 일본 기계(물리)보안 시장 규모 >

□ 주요국 시장동향

▪ 글로벌 시장동향_독일 이스라엘

- 정보보호 기술 개발을 국가 경쟁력 강화의 수단으로 인식, 장기적 투자 시작
  - [독일] 하이테크 2020` 5대 핵심분야에 보안 선정, 연간 GDP의 9.3% 투자
  - [이스라엘] 연간 100억달러 규모 정보보호 R&D 투자 및 JVP 인큐베이터 등 제도 마련

* JVP 인큐베이터 : 중소기업 대상 업무능력 향상을 위한 편의시절 제공

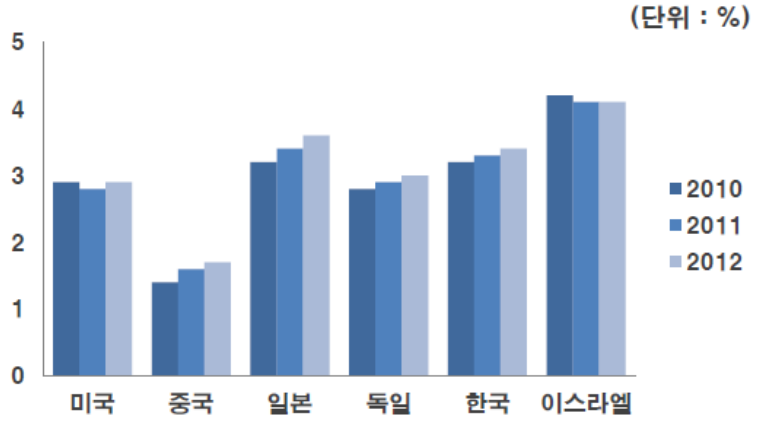
< 하이테크 전략 2020 목표>

- 시민사회 보호/보안 솔루션 연구개발 지원
- 보안 분야 국가기술력 확보 및 관련 연구 인프라 구축
- 안전침해 위기대응 시스템 및 위험방지 솔루션 개발 지원
- 독일의 보안기술 역량 및 시장 경쟁력 강화

< 하이테크 전략 기대효과>

- 효율적인 지식 및 기술 이전
- 중소/중견기업 지원 강화
- 지적재산권 보호 강화
- 창업조건 개선 및 창업 지원

* 출처: 정보보안 글로벌 시장동향, 코트라, 2013

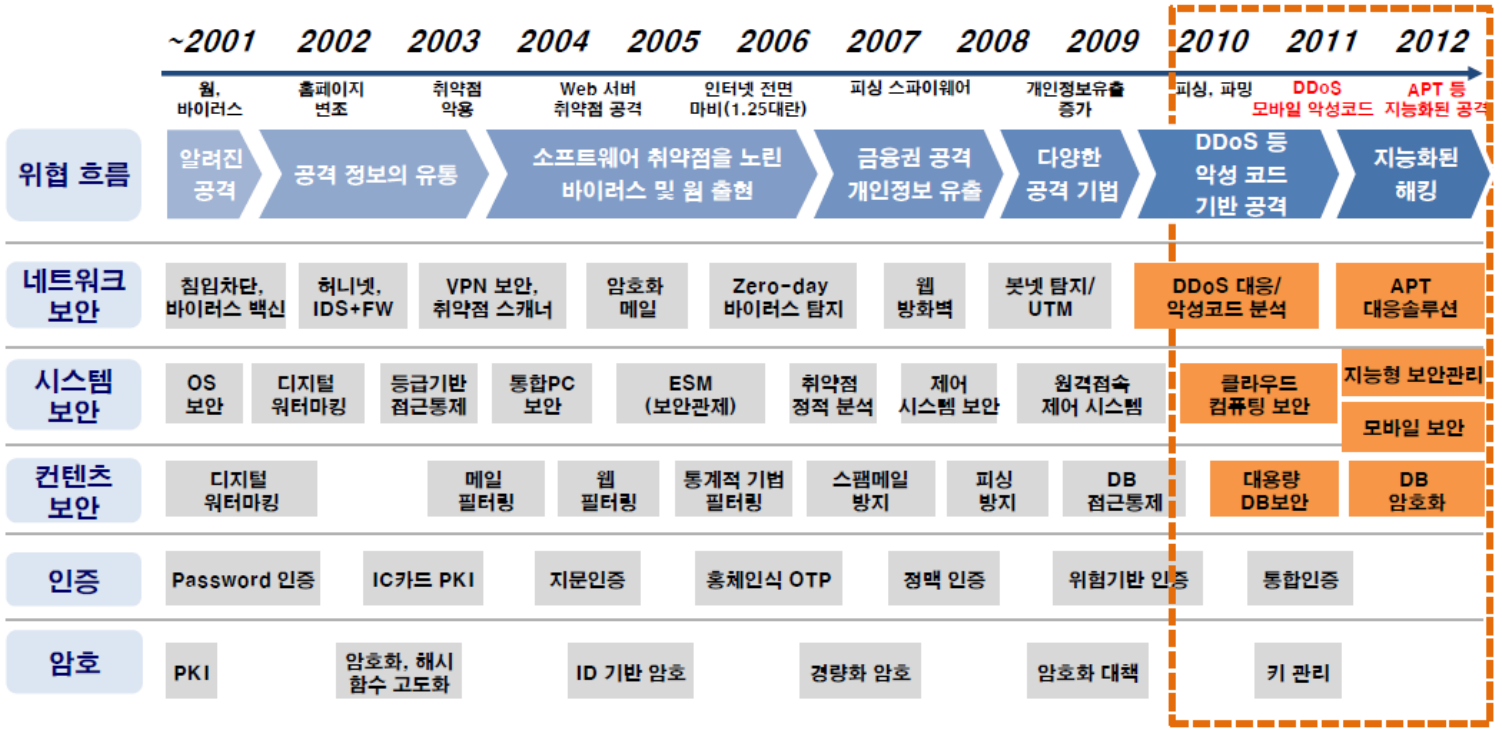


* 출처: Bellette, 2012

< 주요국 GDP 대비 과학기술 R&D 지원 현황>

□ 향후 정보보호기술 전망

- APT 등 신종 공격에 대응, 지능형 보안시장이 크게 성장
  - 지능형 사이버보안을 향후 5~10년간 핵심 사이버 방어기술로 예측
- 지능형 영상감시 등 물리보안 시장 성장
  - 9.11 테러이후 세계적으로 국가안보 전략기술로 인식되어 산업이 빠르게 성장



< 정보보호기술 연구 현황 >

□ 주요 시장 참여자

보안 관제 메이저 기업

기업명	URL	대표자	업체 동향
㈜이글루시큐리티	www.igloosec.co.kr	이득춘	• 사이버보안관련소프트웨어(해킹탐지,보안망 취약점 분석) 개발, 공급, 인터넷보안관리
에스케이인포섹㈜	www.skinfosec.com	한범식	• 소프트웨어(보안솔루션구축, 정보보호컨설팅, 보안관제, 정보침해사고 대응) 개발, 공급, 정보통신교육, 지식인력개발
㈜안랩	www.ahnlab.com	권치중	• 컴퓨터바이러스 연구, 백신프로그램 통합 보안패키지 S/W,보안솔루션, 리눅스, 보안호스팅 개발

보안 관제 신생 기업

기업명	URL	대표자	업체 동향
유넷시스템㈜	unet.kr	심종헌	• 소프트웨어 개발, 공급
㈜윈스	www.wins21.co.kr	김대연	• 컴퓨터프로그래밍, 시스템통합, 관리
㈜에이쓰리	www.a3security.co.kr	한재호	• 정보보안(방화벽, 메일보안) 컨설팅, 솔루션, 소프트웨어(로그분석시스템) 개발, 판매/하드웨어, 통신기기 도소매

SI 기업

기업명	URL	대표자	업체 동향
한전 KDN㈜	www.kdn.com	임수경	• 전력IT시설관리, 소프트웨어 개발, 공급, SI컨설팅, 경영관리시스템 구축, 운영,정보처리/통신설비공사, 전기공사
㈜LG CNS	www.lgcns.co.kr	김대훈	• 시스템통합구축, 소프트웨어 개발, 자료조사처리/물류자동화 컨설팅
롯데정보통신㈜	www.ldcc.co.kr	마용득	• 시스템소프트웨어(SI) 개발, 시스템관련 정보관리/컴퓨터주변기기 도소매

☐ STP 분석

Segmentation

대분류	중분류	소분류
정보서비스업	소프트웨어 개발 및 공급업	시스템 소프트웨어 개발 및 공급업
	컴퓨터 프로그래밍, 시스템 통합 및 관리업	컴퓨터시스템 통합 자문 및 구축 서비스업

Targeting

적용분야	산업 요구사항	타겟기업	
보안 관제 시스템 개발 및 서비스	• 지능형 보안을 지향하는 차세대 보안 정보 분석 기술 필요	대 / 중견기업	에스케이인포섹㈜, ㈜이글루시큐리티, ㈜안랩
		중소기업	㈜에이쓰리, 유넷시스템㈜, ㈜윈스
		대 / 중견기업	한전 KDN㈜, ㈜LG CNS, 롯데정보통신㈜
		중소기업	오픈정보기술㈜, ㈜하우리

Positioning

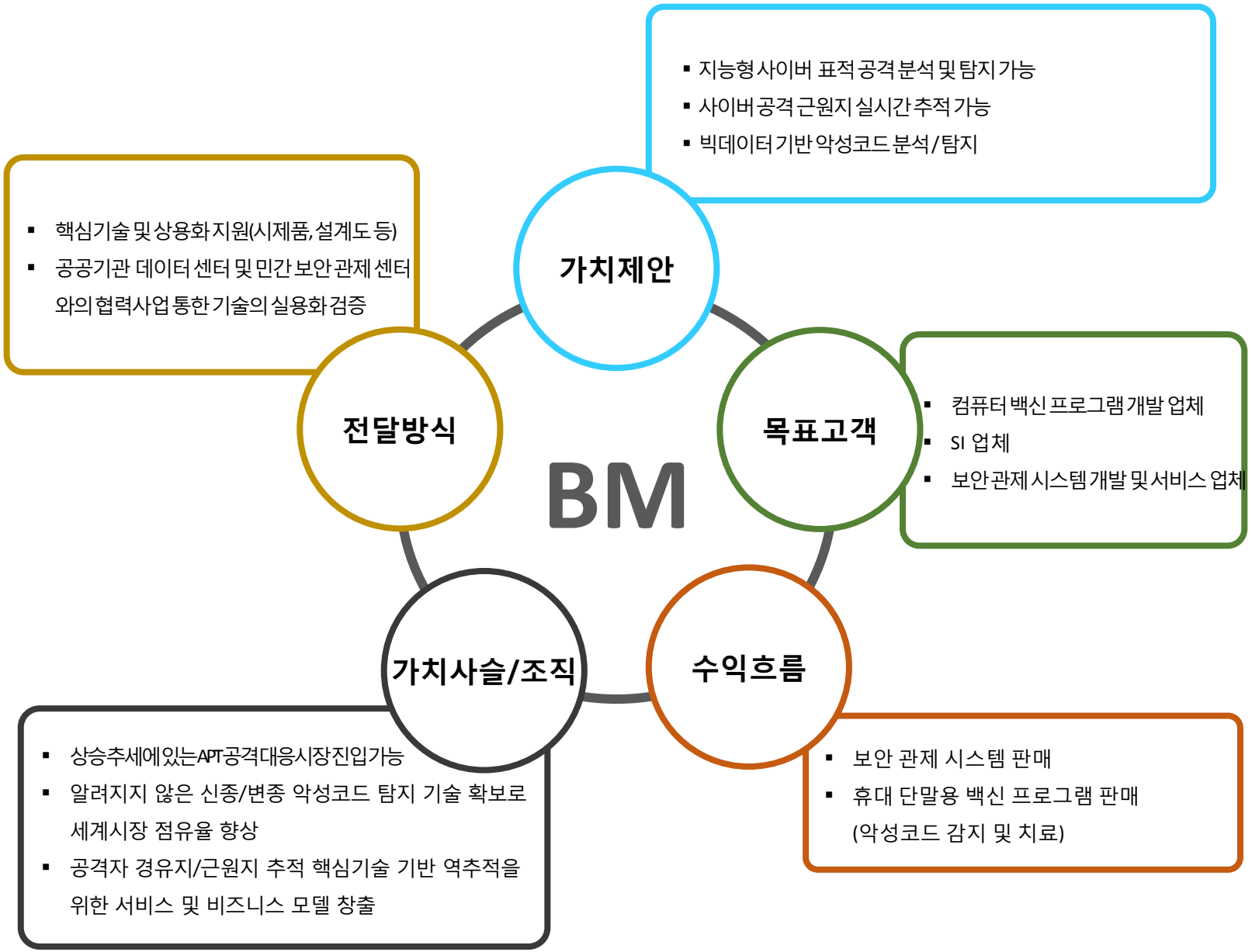
경쟁요소	통합보안시스템	지능형 보안	타겟기업	Selling Point
포지셔닝	높음	높음	㈜안랩, 에스케이인포섹㈜, ㈜이글루시큐리티, ㈜윈스	• SIEM 시장으로 사업영역 확대
	높음	낮음	유넷시스템㈜, 오픈정보기술㈜	• 지능형 보안 시스템 구축 가능 • 제품 경쟁력 강화
	낮음	높음	㈜에이쓰리, ㈜하우리	• 네트워크 전반에 대한 안정성 확보
	낮음	낮음	한전 KDN㈜, ㈜LG CNS, 롯데정보통신㈜	• 기술업그레이드 기반 기술협력 기회 마련

□ SWOT 분석

내부요인		외부요인	
강점 (S)	다양한 장비에서 수집된 로그를 기반으로 행위 분석 수행	기회 (O)	다양한 요구 시장접근 기회 확대
	새로운 형태의 APT 공격 탐지 정확도가 높으며, 다양한 장비의 로그와 연동 가능		폭발적인 관심이 되는 APT 공격 대응시장에 진입
약점 (W)	전체 솔루션 가격이 높음	위기 (T)	침해사고 코드명의 표준화가 완료되지 않아 시장 확대의 어려움
	자체 차단 기능 없음		다수 벤더들(IPS/NGFW/콘텐츠보호)이 해당 솔루션과 경쟁

SO 전략(우선수행)	WO 전략(우선보완)
• 기술이전 실시와 사업화 연계 사업 추진 • 공동연구기관의 사업화 전략 동반 지원	• 단위 모듈로 시장 제품 공략
ST 전략(RISK 해결)	**WT 전략(장기보완)**
• 국내외 표준화 활동 강화	• 국가 기관 보안 센터 시범서비스 통한 실용가능성 검증

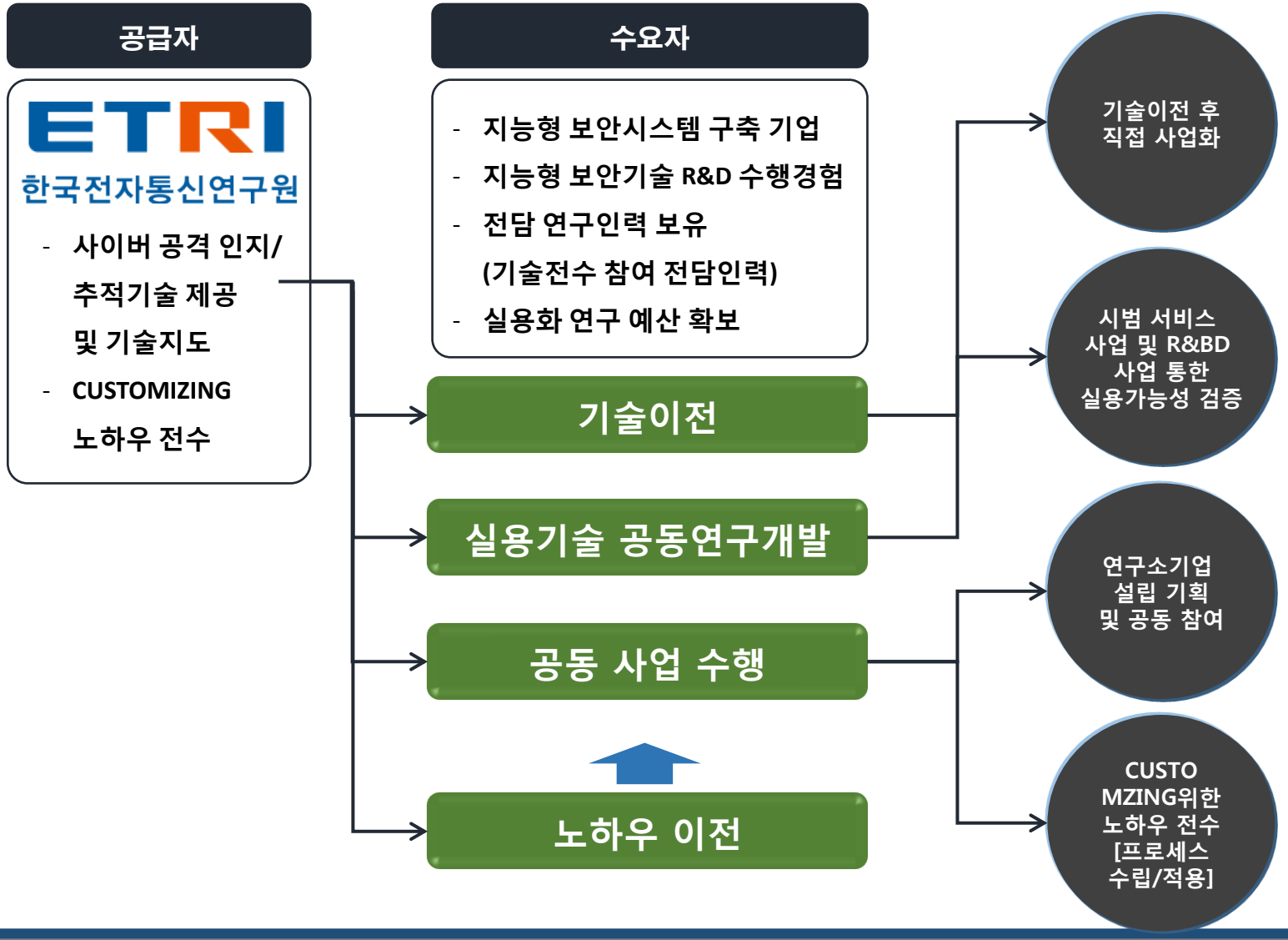
비즈니스모델


BM
가치제안
▪ 지능형 사이버 표적 공격 분석 및 탐지 가능
▪ 사이버 공격 근원지 실시간 추적 가능
▪ 빅데이터 기반 악성코드 분석/탐지
전달방식
▪ 핵심기술 및 상용화 지원(시제품, 설계도 등)
▪ 공공기관 데이터 센터 및 민간 보안 관제 센터와의 협력사업 통한 기술의 실용화 검증
목표고객
▪ 컴퓨터 백신 프로그램 개발 업체
▪ SI 업체
▪ 보안 관제 시스템 개발 및 서비스 업체
가치사슬/조직
▪ 상승추세에있는APT공격대응시장진입가능
▪ 알려지지 않은 신종/변종 악성코드 탐지 기술 확보로 세계시장 점유율 향상
▪ 공격자 경유지/근원지 추적 핵심기술 기반 역추적을 위한 서비스 및 비즈니스 모델 창출
수익흐름
▪ 보안 관제 시스템 판매
▪ 휴대 단말용 백신 프로그램 판매 (악성코드 감지 및 치료)

□ 기술사업화 수익구조


공공 보안 과제 시설
민간 보안관제 센터
테스트 기회 제공
국가사이버 안전센터
사이버 공격 인지 및 추적 기술 제공
기술료
지능형 사이버 공격 인지 및 추적 기술
IT R&D Global Leader
ETRI
INTERNET
지능형 사이버 공격 인지 및 추적 개요
기술료
보안관제 시스템 업체
핵심기술 이전 상용화 지원
제품적용 지원
라우터 / 방화벽 업체
ViRobot
"안전한 인터넷 세상을 위한 선택"
에스케이인포섹(주)
ESTsoft
WINS
IGLOOSECURITY
서비스 판매
수익
수익
제품 판매
최종 소비자

□ 협업 사항


공급자
ETRI
한국전자통신연구원
- 사이버 공격 인지/ 추적기술 제공 및 기술지도
- CUSTOMIZING 노하우 전수
수요자
- 지능형 보안시스템 구축 기업
- 지능형 보안기술 R&D 수행경험
- 전담 연구인력 보유 (기술전수 참여 전담인력)
- 실용화 연구 예산 확보
기술이전
실용기술 공동연구개발
공동 사업 수행
노하우 이전
기술이전 후 직접 사업화
시범 서비스 사업 및 R&BD 사업 통한 실용가능성 검증
연구소기업 설립 기획 및 공동 참여
CUSTOMZING위한 노하우 전수 [프로세스 수립/적용]