지능형공격 대응을 위한 새로운 변화

2014. 4. 24

원 유 재

목 차

Ⅰ 정보보호의 중요성

Ⅱ 현황 및 당면과제

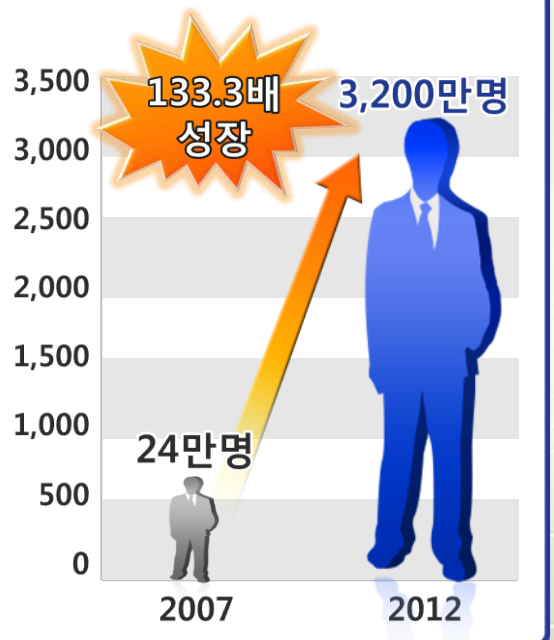
Ⅲ 추진과제

Ⅳ 기대효과

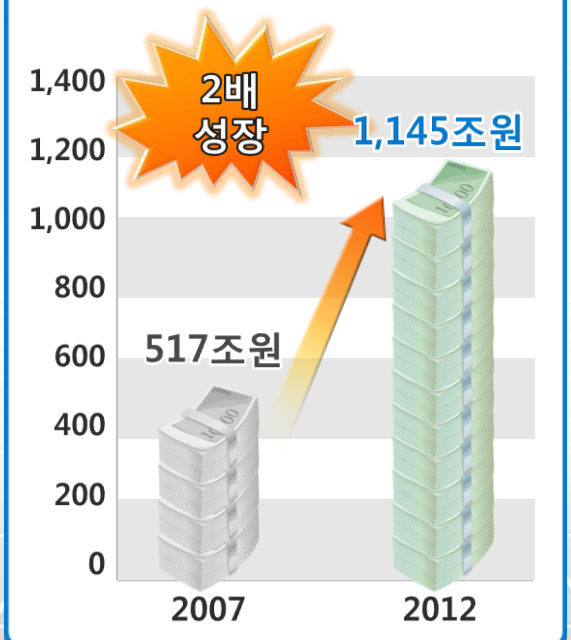
정보보호의 중요성

스마트플랫폼 기반으로 일상생활 全영역에서 ICT에 대한 의존도 심화

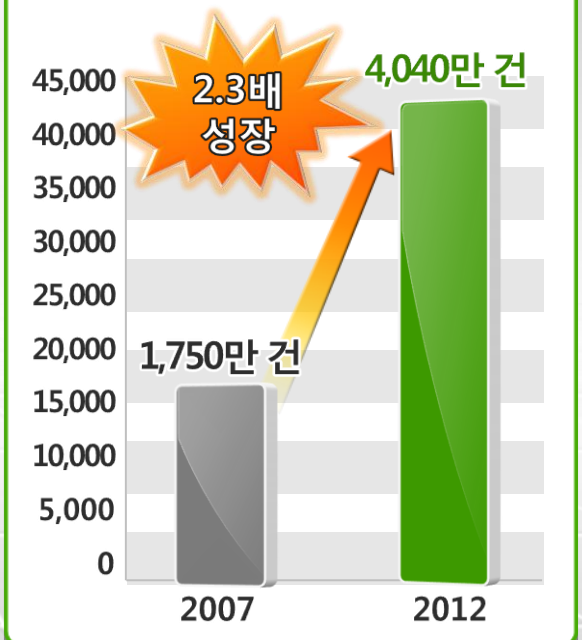
국내 스마트폰 이용자 수



국내 전자상거래 규모



국내 인터넷뱅킹 일평균 이용건수

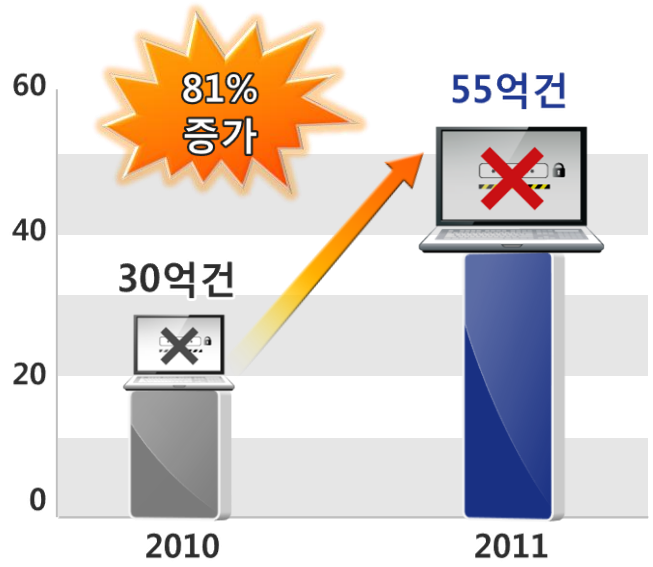


정보보호의 중요성

- 사이버 공간은 실시간으로 연결된 **제2의 현실 세계**

  ➡ 사이버 피해는 현실공간보다 **더 크고 위협적** (사회 안정과 국가 안위로 직결)

세계 '11년 사이버 공격



사이버 범죄로 인한 직간접적 피해

(온라인 금융사기나 아이디 도용 등)

3,880억 달러
(약 417조원) 추정

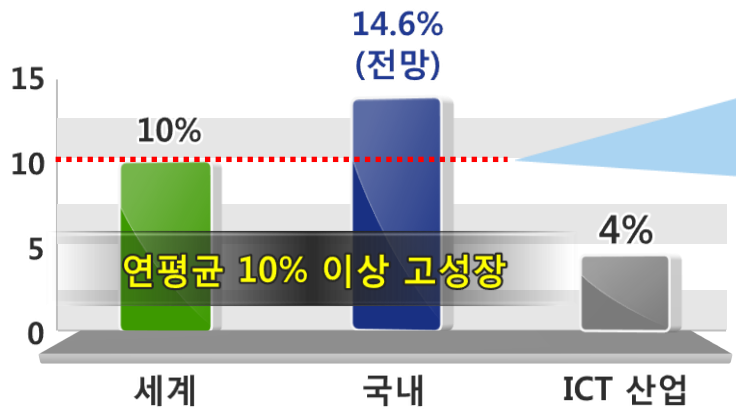
* 국내 3. 20사태('13년)로 일평균 33조원이 거래되는 금융시스템의 일부 마비, 이로 인한 직간접적 피해는 약 **4,400 ~ 8,000억원**으로 추정

정보보호의 중요성

- **사이버 세상의 리더십과 창조경제의 첨병**으로서 정보보호산업을 신성장산업으로 육성

세계 정보보호산업 시장규모('12년)		유무선 통신서비스 시장 규모
1,732억불	=	1,655억불

정보보호산업 성장률



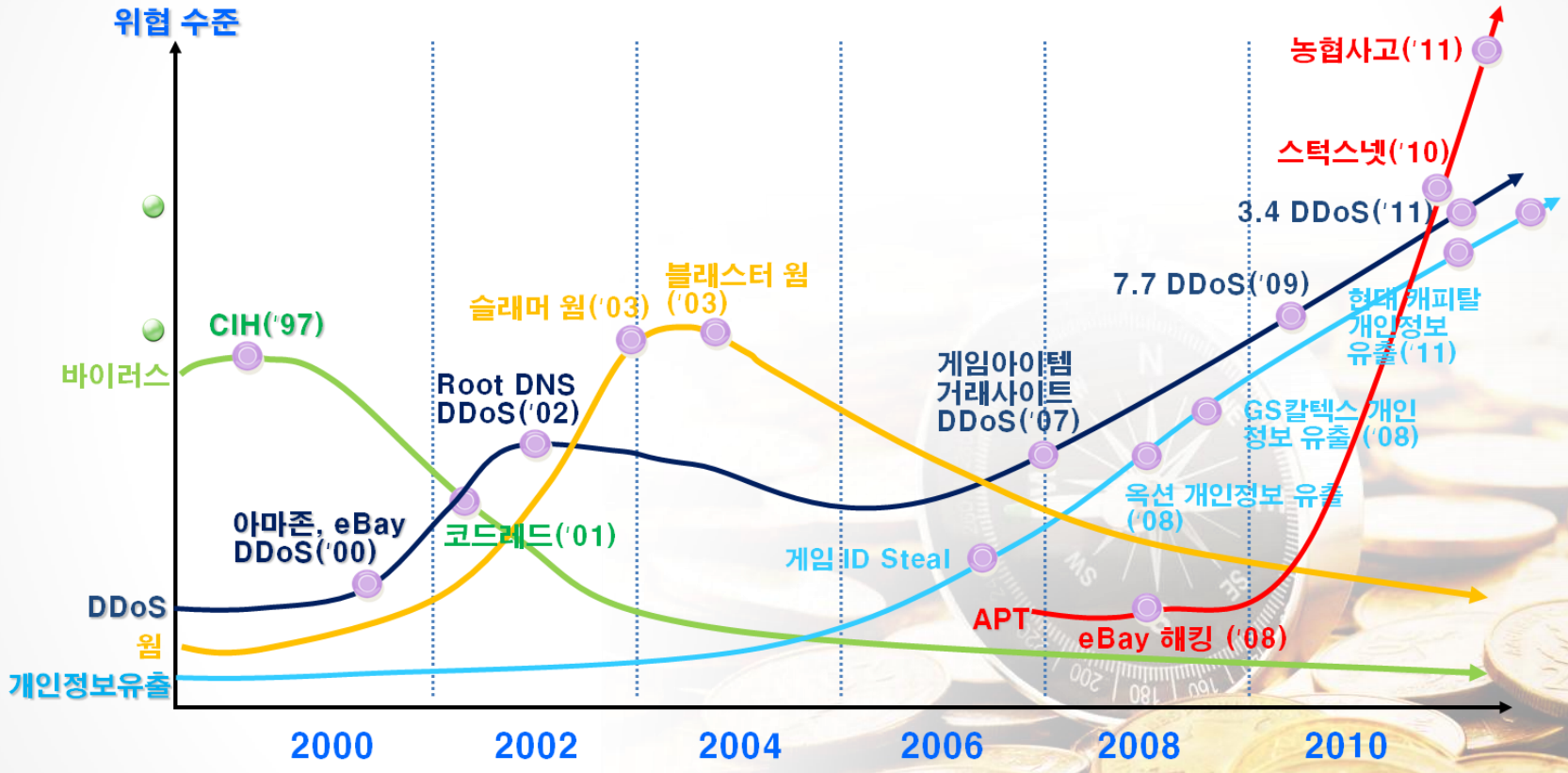
국내는…

지정학적 위험과 ICT 융합 확산에 따른 높은 사이버 위협 요인 등으로 **성장률이 세계시장보다 상회**

정보보호의 중요성

보안위협 증대

☐ 동기 : 호기심, 자기과시 → 금품갈취 → 사회혼란, 사이버테러
☐ 기법 : 수동 → 은닉, 자동화 → 조직적, 지능화



APT(Advanced Persistent Threat) : 명확한 목표물에 대해 장시간 동안 치밀하고 정교하게 공격하는 것

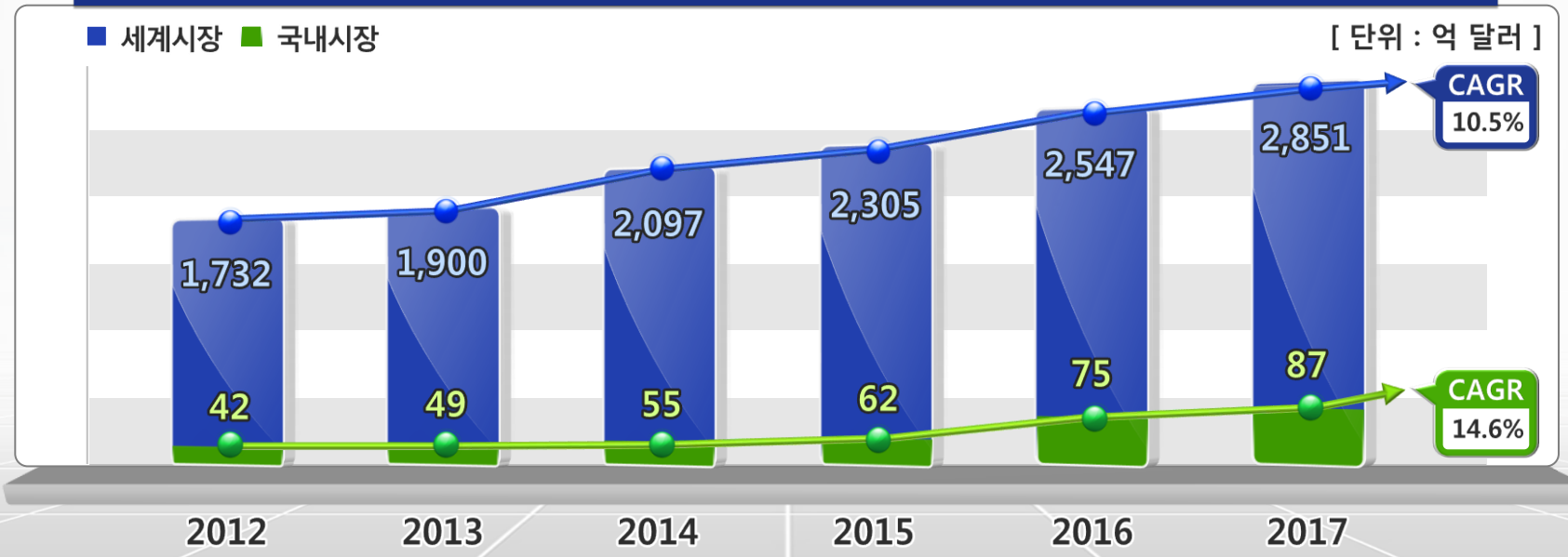
현황 및 당면과제 - 수요측면

시장 협소

- 국내 정보보호시장의 연평균 성장률은 세계시장(10.5%)보다 큰 14.6%로 예상되나 국내 시장은 여전히 **세계시장의 2.4%에 불과** (기업 정보보호 투자 미흡)

※ 국내 IT 시장규모는 세계 IT 시장의 10% 수준

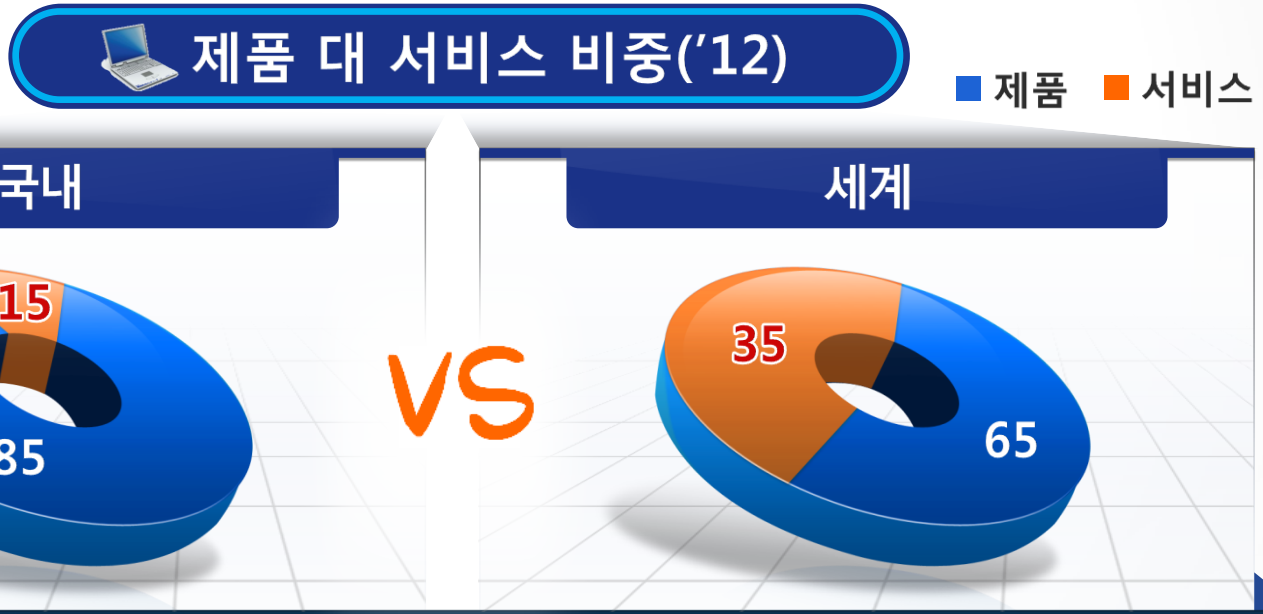
정보보호시장 현황



현황 및 당면과제 - 수요측면

시장 편중

- 미국, EU 등 선진국은 정보보호서비스 중심으로 발전중이나, 국내는 여전히 정보보호 **제품 비중이 너무 큰 후진적 구조**



- 특히, 수요 부문별로는 **공공 및 금융 부문에 편중**된 취약성(50% 육박)

현황 및 당면과제 - 공급측면

기술경쟁력

- 국내기업은 **기초·원천기술 부족**(기술격차 1.6년)으로 혁신적 신규제품 개발보다 시장포화인 기존제품 개선 주력
- 對**미국 기술격차**('11년 79.8%→'13년 79.9%, **0.1%↑**)가 **답보상태**
  - 중국의 對미국 **기술격차('11년 70.6%→'13년 72.7%, 2.1%↑)**는 현격히 감소

GDP차이

정보보호 R&D 투자 규모

현황 및 당면과제 - 공급측면

인력 수급 불균형

- 대학 등 정규교육기관을 통해 연간 800명 이상 배출되나, 대부분 일반적 수준에 머무르고 **우수·현장인력 부족**
  - 인력의 **양적 수급차는 확대, 질적 수급차는 심화**

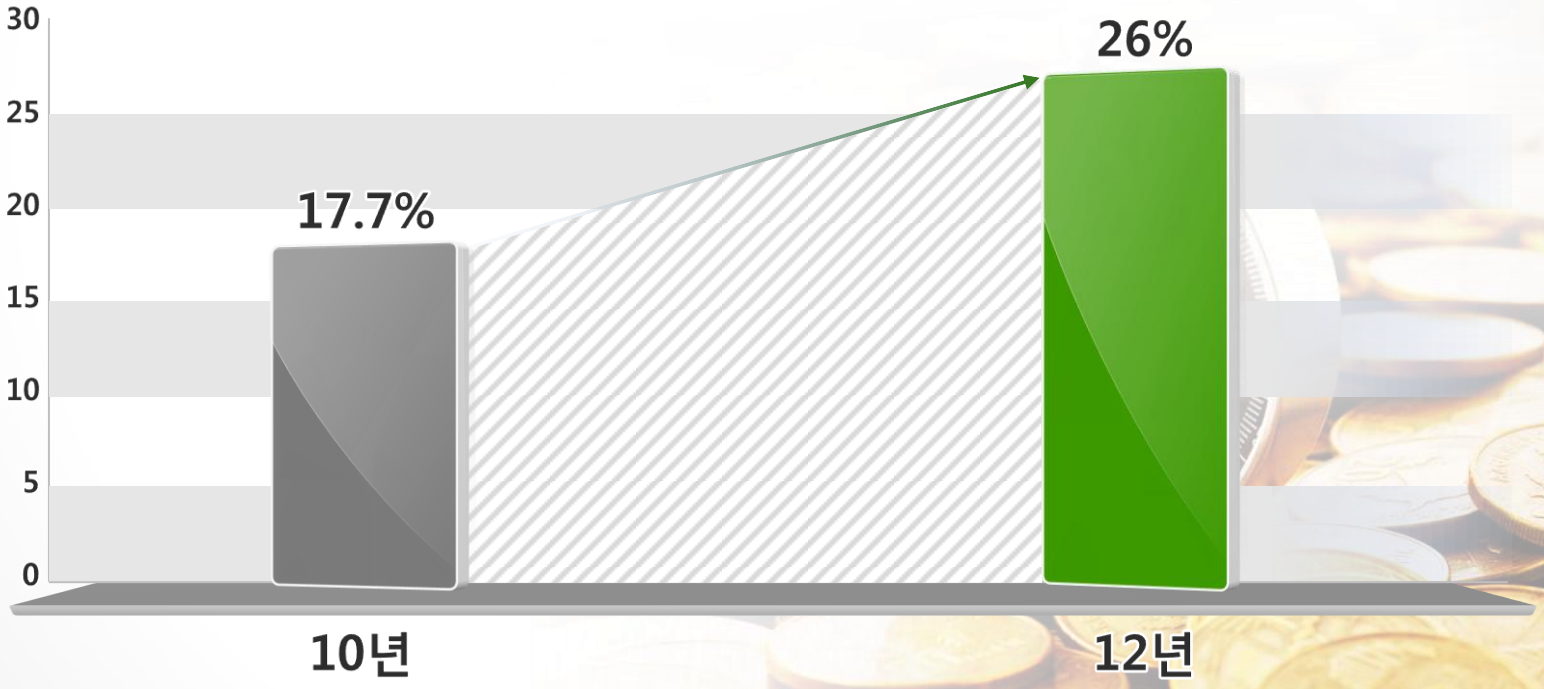
인력 부족분

('12년 실태조사, KISA)

현황 및 당면과제 - 산업구조측면

영세성

- 국내업체의 약 92%(611개)가 매출액 300억 미만의 중소기업으로 산업 및 수출을 리드할 핵심업체 부재
- 경쟁력 부족으로 외국계 기업의 국내시장 점유율이 증가추세



현황 및 당면과제 - 국내시장 제품별 매출특성

시장규모	100억~400억	400억~700억	700억~900억	900억~
<기존 보안위협>	PC 방화벽	**방화벽**(Firewall)	DB 보안(접근제어)	
웜·바이러스	**안티 스파이웨어**	**웹 방화벽**	PC보안	**영상수집장치**
불법접근	**스팸차단**	VPN	DRM	(DVR)
DDoS	**보안운영체제**	**공인/사설 인**	**침입방지**	**카메라**(CCTV)
불법 스팸	**싱글사인온**(SSO)	**비스**	**바이러스 백신**	**엔진/칩셋**(영상)
웹 해킹	DDoS 대응	**통합보안관리**	**보안관제**	
		PKI		
<지능형/신규 보안위협>	**취약점 분석 도구**			
	로그관리 분석 도구			
무선/모바일 위협	**무선네트워크 보안***		**영상감시 관리**	
지능형 공격(APT)	**모바일 보안***	DB 암호*	**영상감시 지능형**	
사이버 사기	**보안 USB**	**얼굴 인식**	**솔루션**	
개인/기업정보 탈취	**보안 스마트카드**		**사회기반시설 보안**	
사회안전 위협	**홍채인식**			
	유해콘텐츠 차단			

현재

앞으로

추진과제 - 정보보호 10대 핵심기술 개발

구분	사이버 위협 대응	ICT 환경변화 대응	범죄예방, 사회 안전	개인정보침해 위협
수출주도형	① APT 공격 대응 ② 사이버블랙박스		③ 지능형 영상감시 ④ 사용자 진화형 얼굴-홍채 인식 ⑤ 유해콘텐츠 차단	
수입대체형		⑥ 무선침입탐지 ⑦ 스마트단말 보안칩 ⑧ 산업용 통합보안		
미래성장형			⑨ Cipherbase 기반 암호 ⑩ 유니버셜 인증	

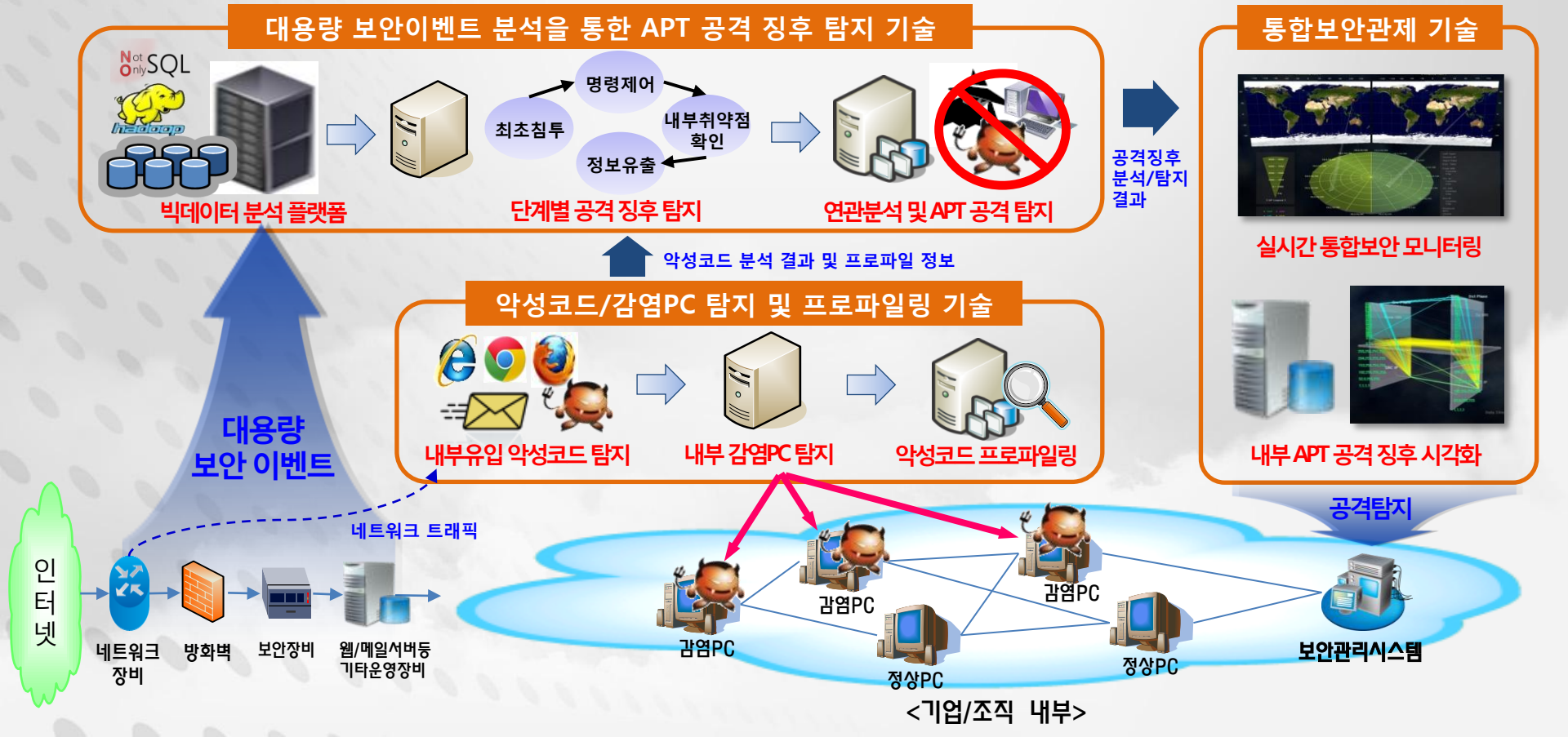
추진과제 – APT 공격 대응 기술

- 기존의 백신이나 네트워크 보안 제품들은 알려지지 않은 공격과 표적 공격을 탐지하는데 시차가 존재함
- 악성코드 특징과 네트워크 트래픽 등의 대용량 사이버 정보들을 빅데이터 마이닝 분석으로 공격징후를 예측하여 공격 사전인지 기술 실현
- 하이엔드 네트워크 보안 핵심기술을 확보하여 글로벌 대표기업과 경쟁할 수 있는 환경 마련

과제명

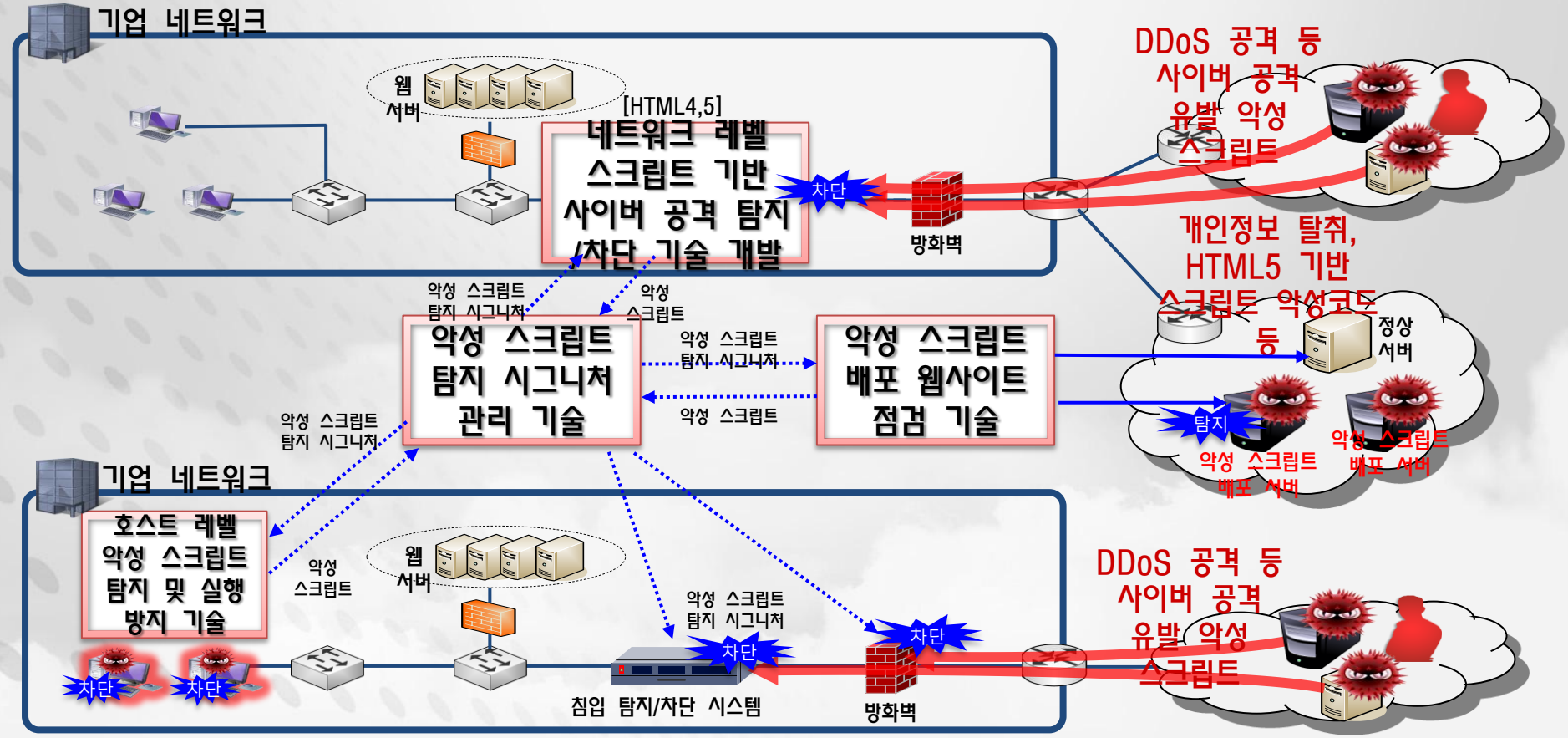
악성코드 프로파일링 및 대용량 보안이벤트 분석을 통한 공격징후 탐지기술 개발

- **(목표) 기업/조직 내부의 정보보호를 위한 빅데이터 분석 기반 고도화된 APT 공격 탐지 기술 개발**
  - 내부로 유입되는 악성코드 및 내부 감염PC 탐지, 악성코드 공격 프로파일링 기술 개발
  - 빅데이터 분석 플랫폼 기반 대용량 보안이벤트 처리 및 APT 공격 징후 탐지 기술 개발
  - 내부 APT 공격징후 시각화 및 통합 보안관제 기술 개발
- **(EndProduct/적용범위) 보안업체에서 개발되는 상용 솔루션/장비 및 일반 기업/조직에서 운영되는 보안관제 시스템 등에 광범위하게 적용**



과제명 스크립트 기반 사이버 공격 사전 예방 및 대응기술 개발

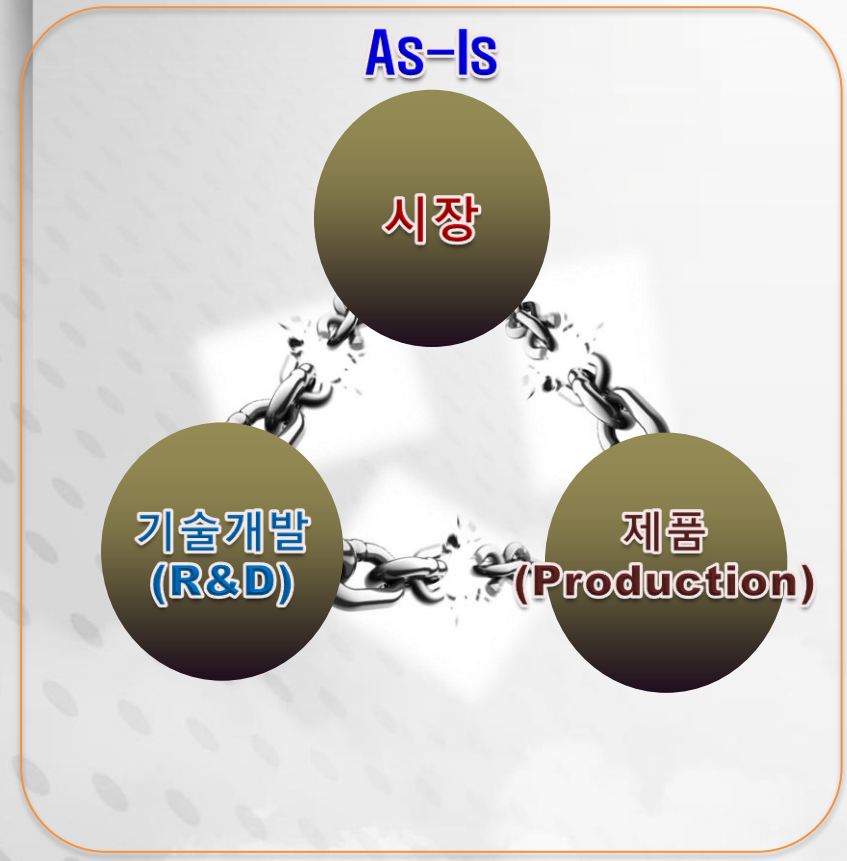
- **(목표)** 악성 스크립트를 이용한 사이버 공격을 예방하기 위한 악성스크립트 탐지 및 실행 방기 기술 개발
  - 네트워크 레벨 스크립트 기반 사이버 공격 차단 기술
  - 호스트 레벨 악성 스크립트 탐지/실행 방지 기술
  - 악성 스크립트 탐지 시그니처 관리 및 웹사이트 점검 기술
- **(EndProduct/적용범위)** 보안업체에서 개발되는 상용 솔루션/장비 및 일반 기업/조직에서 운영되는 보안 관제 시스템 등에 광범위하게 적용

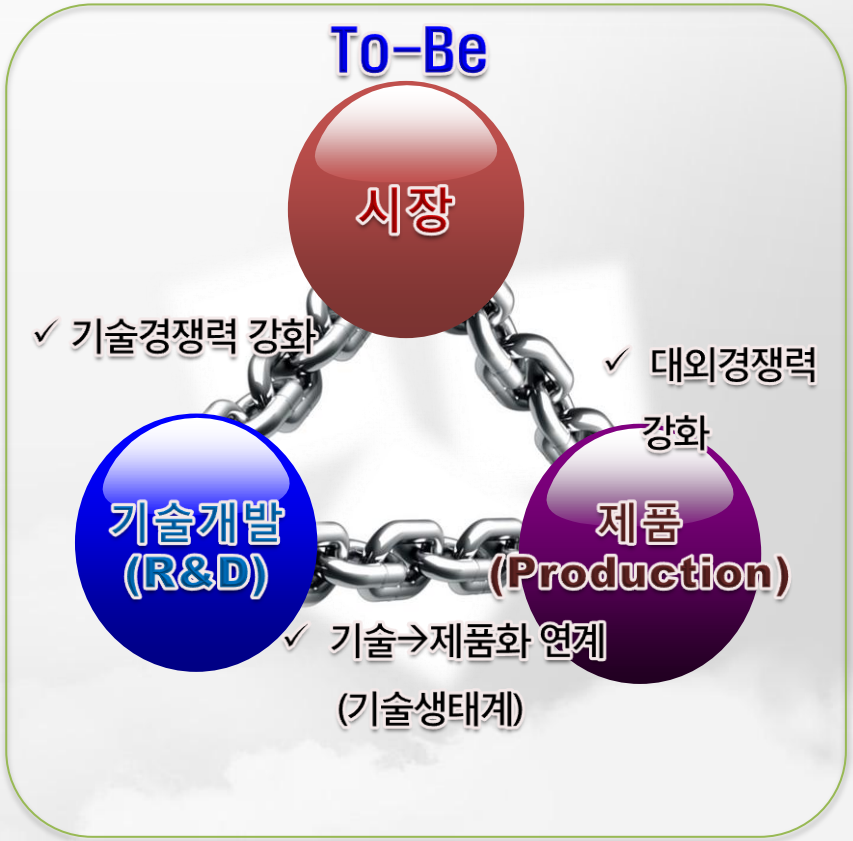


추진과제 – 사이버 블랙박스 기술

- 침해사고 증거보존이 안되어 사고분석 시간이 장기간 소요되고 타 기관의 사고가 내부 조직에 미치는 영향분석이 불가능
- 사이버 침해사고 증거보존 및 재현이 가능하고 전문 관리자가 사고 연관성 분석을 통한 징후 인지 등의 업무를 수시로 분석할 수 있는 작업환경 제공
- 사이버 침해사고 대응을 통합적인 보안 서비스로 끌어올리고 해커의 작업환경과 같은 대응 환경 조성

기대효과


As-Is
시장
기술개발
(R&D)
제품
(Production)


To-Be
시장
✓ 기술경쟁력 강화
✓ 대외경쟁력
강화
기술개발
(R&D)
제품
(Production)
✓ 기술→제품화 연계
(기술생태계)

감사합니다