7.7 DDoS 공격 대응조치 및 기업정보보호 수준제고 방안

'09. 9. 17.

방송통신위원회
KOREA COMMUNICATIONS COMMISSION

목 차

I. 추진 배경 – 7·7 DDoS 경과 및 대응조치

- '09년 7.7일부터 대규모 조직적 DDoS 공격 발생
  - 공공기관, 언론사 등 주요 웹사이트에 대해 조직적 공격으로 인터넷 접속 장애 발생
    - ※ 1차 : 26개(국내 12개), 2차 : 16개(국내 15개), 3차 : 7개(국내 7개)
  - 특정 사이트의 일시적 접속장애로 일부 기업의 이미지 실추, 국민불편 등 피해 발생

- 1.25대란 이후 인터넷모니터링 체계구축 등을 통해 침해사고는 감소하였으나,
  - 새로운 사이버 위협의 출현에 따라 정부와 관련기관의 대응만으로는 한계에 봉착
  - 신규서비스가 확산되는 시점에는 더욱 다양하고 심각한 공격 예상
    - ※ IPTV용 셋탑박스가 악성코드에 감염될 경우, DDoS 공격의 파괴력 심화

일상화·조직화되고 있는 사이버 공격의 선제적 예방 및 조기 차단을 위한 민간 사이버보안 강화가 필요

<참고> DDoS 공격 대상 사이트

공격차수			기 관 명				비고
1차	2차	3차					
■	■		청와대	국방부			국내(22개 사이트)
■			외교통상부	국회	한나라당	네이버(블로그)	
■			농협	신한은행	외환은행		
	■	■	전자민원G4C	다음(메일)	파란(메일)	국민은행	
	■		NCSC	기업은행	하나은행	우리은행	
	■		알툴즈	안철수연구소			
■	■	■	옥션	조선일보	네이버(메일)		
■	■		한미연합군사령부				미국(14개 사이트)
■			백악관	국무부	국방부	재무부	
■			국토안보부	연방항공국	뉴욕증권거래소	나스닥증권거래소	
■			U.S. Bank	야후	VOA	워싱턴포스트	
■			U.S. auctions live				

I. 추진 배경 – 7·7 DDoS 경과 및 대응조치

◆ 정부는 당정협의를 거쳐 국가사이버위기 종합대책을 마련
◆ 국가사이버안전전략회의에서 심의 · 확정

(국가기관간 기능 조정) 국정원은 사이버위기 대응업무 총괄, 방통위는 민간 분야 사이버 공격 대응 및 대언론 창구역할 담당 등

(당면과제) 사이버위기관리체계 강화, 악성프로그램 삭제요청권 및 침해사고 발생시의 시스템 접근요청권 등의 법적 근거 마련, 국가위기관리기본지침 개정 등

(2010년 완수과제) 정부 사이버위기 대응조직 강화, 공공부문 업무망 · 인터넷망 분리 사업 확대, 사이버공격 탐지 사각지대 해소 등

(중장기 과제) '한국인터넷진흥원' 인력보강 등 사이버 전문인력 양성, 정보보호예산의 단계적 확대, 정보보호산업 육성 지원 등

◆ 방송통신위원회는 보도자료 배포를 통해 정부 종합대책을 홍보(9.14)
◆ 10월 중 방통위 차원의 DDoS 등 사이버대응 세부실행계획 마련

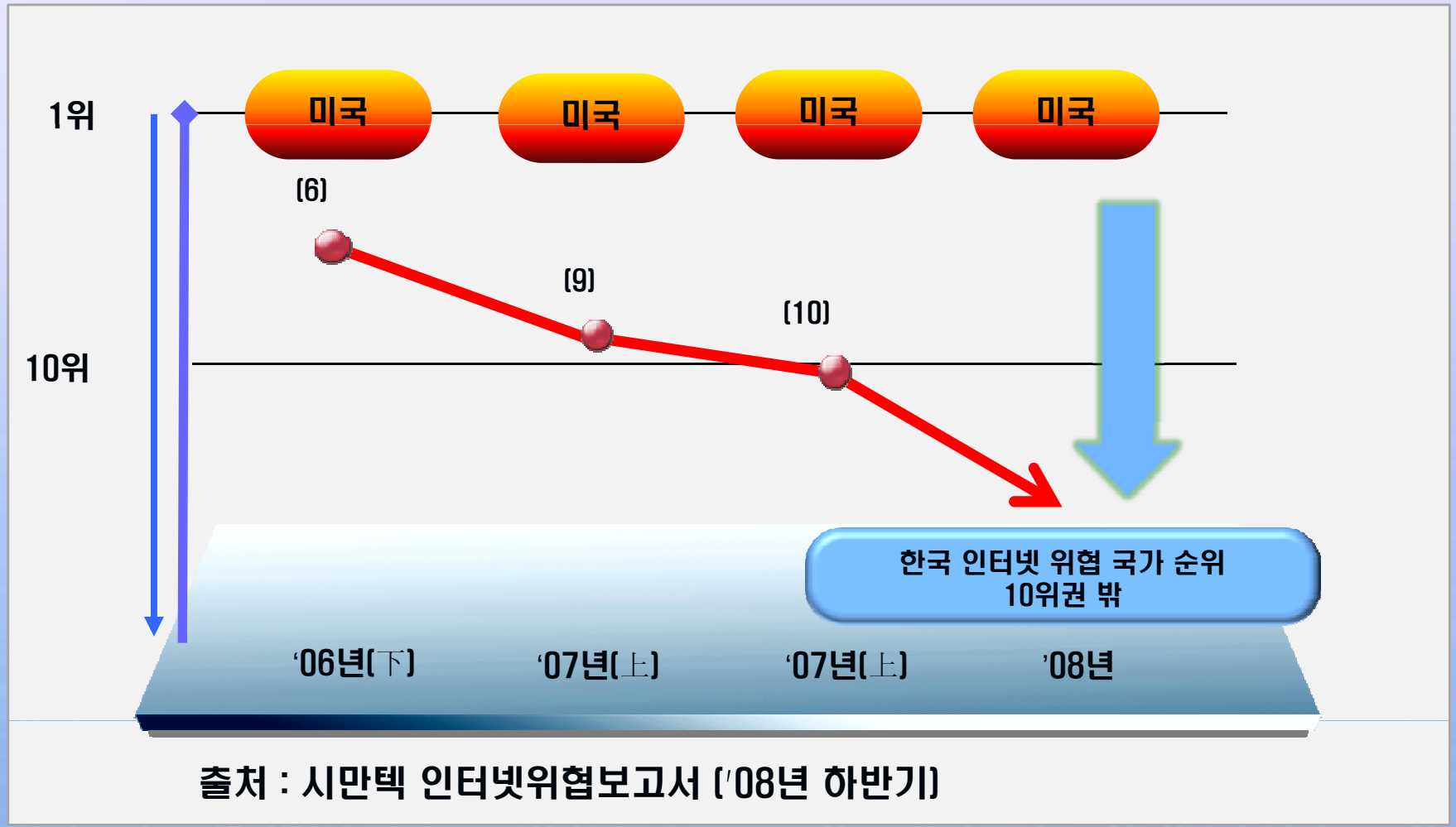
I. 추진 배경 – 그간 정보보호정책 추진 성과 (1)

◆1.25 이후 정보통신망법 개정, 대응지원센터 설립 운영('03.11~현재)

- 정보통신망법 개정
  - 인터넷침해사고 긴급대응 업무수행 근거마련 (한국정보보호진흥원)
  - ISP의 이상트래픽 정보제공, 침해사고 신고의무화
- KISA 인터넷침해대응센터(KISC) 설립/운영('03~)
  - 24시간 상시 모니터링 및 대응, ISP로부터 정보수집 (163개 기관)
  - "제2의 1.25침해사고" 재발방지 목표(긴급 트래픽 차단체계)
- 네트워크 이용자보호 기능강화('05~)
  - 악성코드 자동 탐지시스템, 악성 봇 싱크홀 등 침해대응기술 개발/적용
  - 국내 ISP(KT, LG데이콤 등)와 공동모의훈련(분기별), 공조체제 강화
  - 해외 아.태 침해사고대응팀 협의회, FIRST 등 국제협력 체계 구축

I. 추진 배경 – 그간 정보보호정책 추진 성과 (2)

◆ 인터넷 위협 국가순위 10위권 밖으로 개선



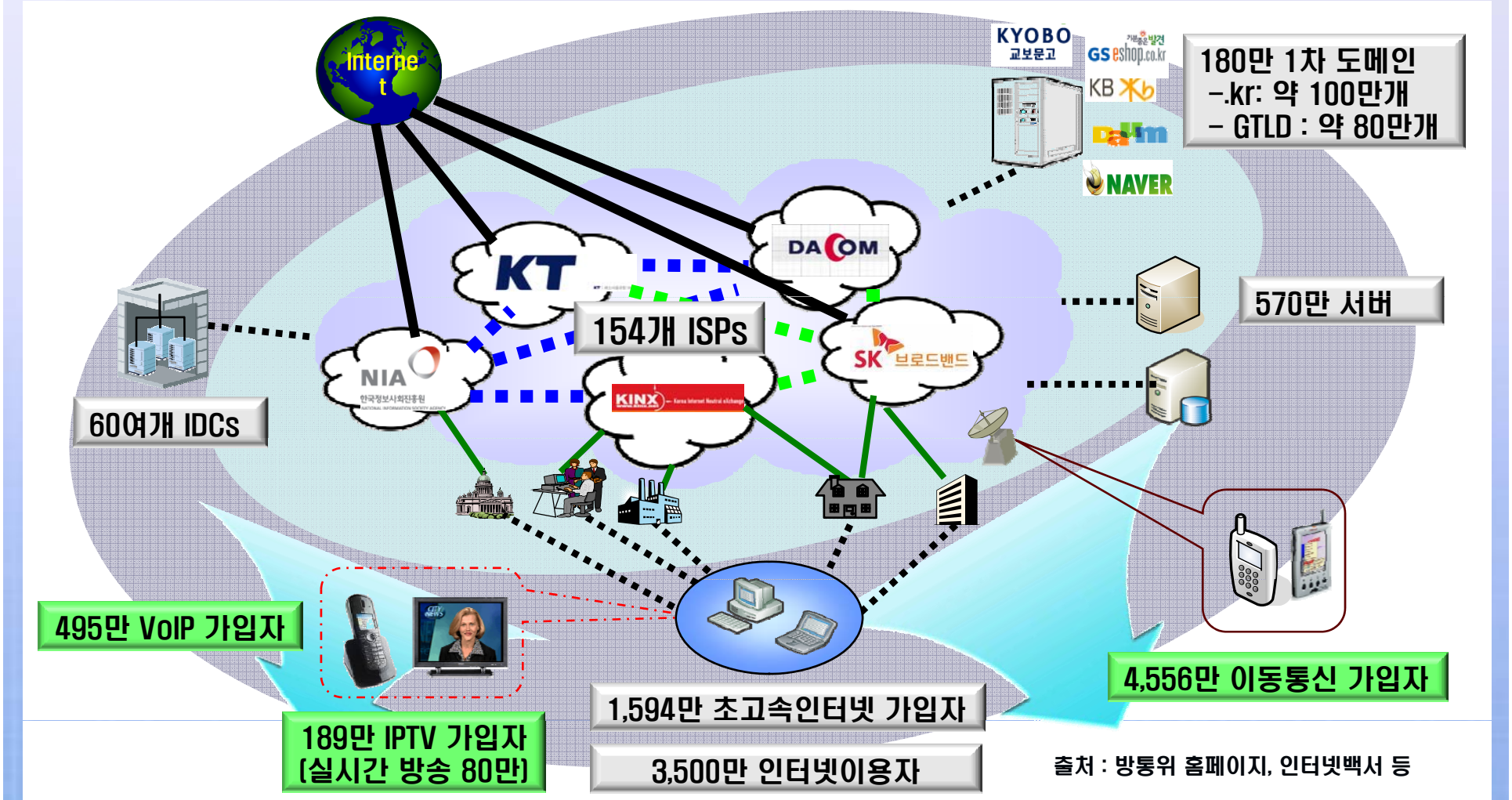
출처 : 시만텍 인터넷위협보고서 ('08년 하반기)

〈참고〉 방통위 정보통신망법상 정책수단

	정책수단	주요 내용	법적근거	비 고
사전예방	정보통신서비스제공자 보호 조치 마련	o ISP가 정보통신망 보호조치를 마련하도록 의무화 - 방통위는 정보보호지침 고시 및 준수를 권고	망법45조	
	집적정보통신시설의 보호	o IDC는 시설의 안정적 운영을 위한 보호조치 마련 의무화 - 방통위는 보호조치의 구체적 기준을 정하여 고시	망법46조	
	정보보호 안전진단	o ISP, IDC 등에 대하여 매년 정보보호안전진단 의무화	망법45조 망법46의3	1천만원 이하 과태료
	정보보호관리체계인증	o 정보보호관리체계 인증기관을 지정 및 인증에 관한 기준 고시	망법47조	
	침해행위 처벌	o 망법 48조1항 위반시 3년이하 징역 또는 3천만원 이하 벌금 o 망법 48조2.3항 위반시 5년이하 징역 또는 5천만원 이하 벌금	망법72조 망법71조	해킹 바이러스 유포 등
사후대응	네트워크 모니터링	o 국내 인터넷망 트래픽 동향 24시간 모니터링 o 주요 ISP, IDC 등이 침해사고 관련 정보 제공 의무화	망법48조의2	1,000만원 이하 과태료
	예.경보 발령	o 관심, 주의, 경계, 심각의 4단계 경보 발령 o 언론 및 정보통신서비스제공자의 전파 의무화	망법48조의2 시행령56조	
	침해사고 신고의무화	o ISP, IDC 등에 대해 침해사고 신고 의무화	망법48조의3	
	대응조치	o 주요 ISP, IDC에게 접속경로 차단요청 o S/W사업자에 대한 보안 취약점 보완 프로그램 제작 요청 o 민.관합동조사단 구성.운영(원인분석과 재발방지대책 수립)	시행령56조 망법48조의4	1,000만원 이하 과태료 2년 이하의 징역 또는 1천만원 이하 벌금

I. 추진 배경 – 민간부문 정보보호 대상

◆ 인터넷 환경 변화에 따른 정보보호 대상 확대



출처 : 방통위 홈페이지, 인터넷백서 등

<참고> '03년과 '09년 인터넷 이용현황 비교

구 분		1.25사태 당시 (2002년 말)	현 재 (2008년 말 기준)	증 가 (증가율)
인터넷 이용자수		26,270천명	35,360천명	9,090천명 (35%)
인터넷 이용률		59.4%	77.1%	17.7%P (30%)
가구 인터넷 접속율		68.8%	80.6%	11.8%P (17%)
초고속인터넷 가입자		7,806천명	15,475천명	7,669천명 (98%)
인터넷 평균 속도	업로드	0.859Mbps	77.639Mbps	76.780Mbps (8,938%)
	다운로드	15.711Mbps	83.523Mbps	67.752Mbps (431%)
국내 인터넷 트래픽		199Gbps	2,520Gbps	2,321Gbps (1,166%)
국가 도메인 수(.kr)		51만개	101만개	50만개 (98%)
IP 갯수		3,098만개	7,224만개	4,126만개 (133%)
전자상거래 시장		178조원	630조원	452조원 (254%)
인터넷 뱅킹 서비스	등록 고객 수	1,771만명	5,260만명	3,489만명 (197%)
	건수(조회포함)	588.5만건	2,242.5만건	1,654만건 (281%)
	금액	7조 1,107억원	22조 8,585억원	157478억원 (222%)
전자민원 (G4C신청건수)		5만건	1,824만건	1,819만건 (36,380%)

I. 추진 배경 – 민간부문 정보보호의 중요성

민간부문의 특성

- 보호대상 방대(전체의 95%)
- 다양 · 다수의 취약점 존재
- 규율시 법적 근거 必要

대응시 주의점

- 정교하고 세심한 정책 · 제도, 고급전문인력, 첨단장비 등으로 대응해야 함

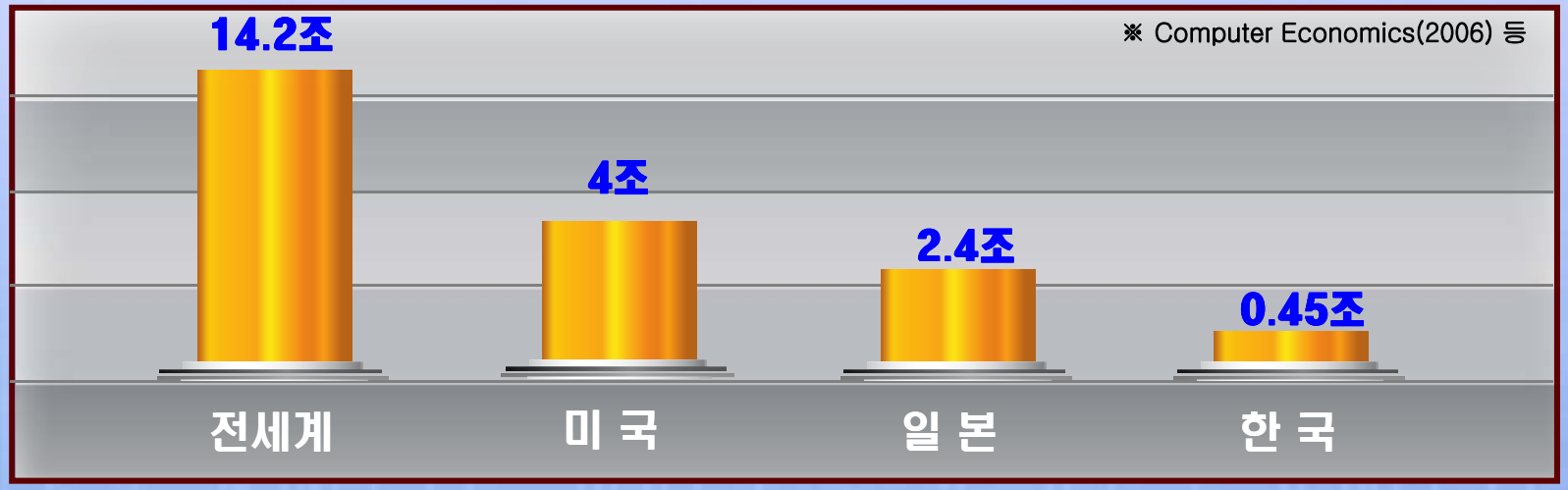
Ⅱ. 정보보호의 경제적 효과 – 경제적 손실(1)

기업부문: 인터넷 침해사고로 인한 경제적 손실

- 웜·바이러스 등 인터넷 침해사고로 인해 매년 국내 기업에서 4~5천억원 정도의 손실 발생

연간 피해손실 및 단일사고 피해손실

- 인터넷 침해사고로 인한 국내 기업의 연간손실액: '05년 4,500억원
- 2003년 발생한 1.25 인터넷 침해사고의 경우, 단일 사고로만 약 1,700억원의 손실 발생



[2005년 기업의 연간 피해액]

Ⅱ. 정보보호의 경제적 효과 – 경제적 손실(2)

가구 부문 : 인터넷 침해사고로 인한 경제적 손실

- '07년 미국 인터넷 이용 가구의 인터넷 침해사고 피해액은 **약 50억 달러(5조원)**

  ※미국 Consumer Report지가 미국 내 인터넷 이용 2,030 가구를 대상으로 실시한 설문 조사 결과

- 미국과 같은 기준으로 측정한 우리나라 가구의 침해사고 피해액은 **약 1조 6천억 원**

한-미 가구 부문 총 피해액

피해액 측정

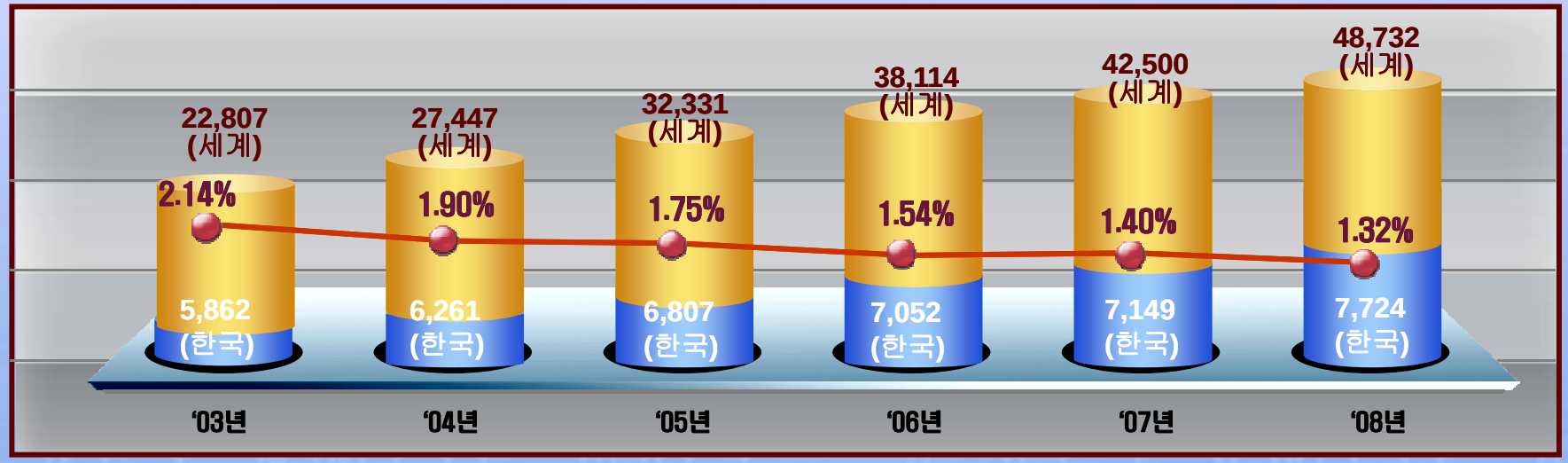
- 미국 Consumer Report지는 **바이러스, 스파이웨어에 의한 건당 피해액을 $100**로 적용하여 산출
- 한국은 **건당 10만원**을 적용하여 총 피해액 산출

Ⅱ. 정보보호의 경제적 효과 – 정보보호시장

고성장하는 국내외 정보보호 시장

- 세계정보보호시장은 과거 6년간 연평균 16.4%의 고성장을 지속하였고, '12년까지 연평균 14% 성장하여 연 818억 달러 수준 형성 전망
- 국내 정보보호시장은 과거 6년간 연평균 5.67%의 성장으로 세계정보보호시장 성장률(16.4%)에 비해 1/3 수준에 불과

[국내 및 세계 정보보호산업 규모 및 성장률 ('03~'08)]



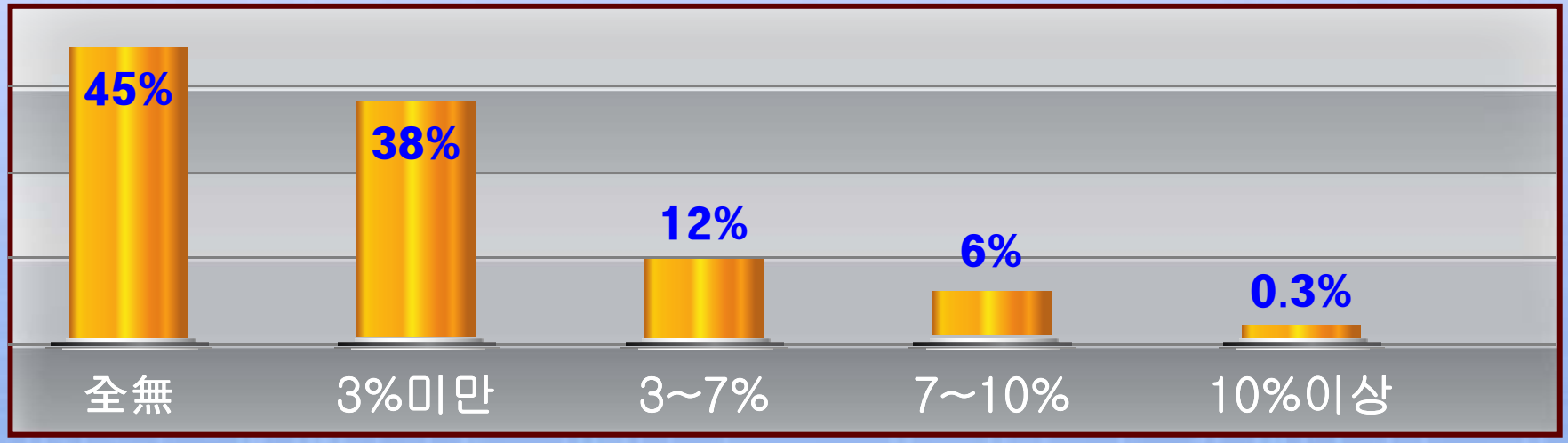
※ 출처 : 세계시장 IDC (단위 : 백만달러)
국내시장 KISA (단위 : 억원)
환율 : 1200원/1달러 기준

Ⅱ. 정보보호의 경제적 효과 – 정보보호투자

증가하는 위협과 달리 감소하는 민간 정보보호투자

- 국내 기업의 연간 정보화 투자총액 대비 정보보호 관련 투자 비율은 전체기업의 80% 이상이 3% 미만 수준
- 기업은 IT를 활용한 서비스 개발, 생산성 향상에 중점을 두고 있으며, 상대적으로 사고 예방 및 대응 투자에 대한 인식이 열악

[민간기업 정보화대비 정보보호 투자현황]



※ 출처 : KISA 2008 정보보호실태조사

Ⅲ. 일반 정보보호 수준제고 방안-대응체계 강화

네트워크

- DDoS 대응시스템 시범구축 확대
  - 인터넷 상의 악성 트래픽 조기 탐지 및 정화 서비스 제공 확대
    - ※ 2% 규모를 10%로 확대하고 나머지 90%는 ISP의 자율적 투자 유도
- DDoS 긴급 대피소(ERS : Emergency Rescue Service) 구축 및 운영
  - DDoS 대응이 취약한 중소업체가 일시적으로 공격을 피할 수 있도록 환경 제공

홈페이지

- 홈페이지 개발 과정부터 해킹 원인을 제거 후 서비스되도록 상시 보안체계 수립
  - ※ 홈페이지 개발 (해킹탐지 및 방지 도구적용) → 홈페이지 개설 (취약점 점검)
  - → 홈페이지 운영 (악성코드 삽입여부 점검)
- 약 180만개의 국내 홈페이지 전체로 악성코드 은닉여부 일일 점검을 확대
  - ※ 현재 일일 점검 홈페이지 수 : 약 15만개

Ⅲ. 일반 정보보호 수준제고 방안-대응체계 강화

이용자 PC

- 전용백신 보급 체계 구축
  - 침해사고 발생 시 공격(홈페이지 DDoS 공격 등)을 유발하는 악성코드를 신속하게 제거
- 선제적 예방차원의 사이버 검역체계 도입
  - 악성코드에 감염된 PC는 인터넷 접속 전에 치료할 수 있도록 사이버 보건소(전용백신 보급 홈페이지)로 자동 접속

KISC 고도화

- 민간부문 총괄인 인터넷침해대응센터가 세계 최고의 침해사고 예방 및 대응 조직이 될 수 있도록 시설증설 및 인력확대

Ⅲ. 일반 정보보호 수준제고 방안-대응체계 강화

침해대응 관련 법제도 제 · 개정

- 고도화된 사이버공격에 선제적 대응을 위한 '정보통신망법' 전부개정안의 조속한 국회통과
  - 사고 분석을 위해 감염 홈페이지에 접근 요청 (시스템 접근 요청권)
  - 악성프로그램이 은닉된 홈페이지 운영자에게 악성프로그램 삭제 요청 등 (악성프로그램 삭제 요청권)

- 좀비PC를 통한 악성프로그램 확산 방지를 위해 가칭 '악성프로그램 확산 방지 등에 관한 법률' 제정 필요
  - 인터넷이용자의 보안프로그램 설치 및 업데이트 권장
  - 긴급한 경우 좀비 PC의 인터넷접속 제한 검토 등

Ⅳ. 기업 정보보호 수준제고 방안 – 기존제도 강화

기존제도 강화

신규제도 추진

투자환경 조성

정보보호 안전진단대상자 확대 추진

- 중.소규모 기업의 정보통신망에 대한 안정성.신뢰성 제고를 위하여 안전진단대상자 선정기준을 강화

  ※ 정보통신 매출액 100억 → 50억, 이용자수 100만명 → 10만명)

- 획일적인 기준으로 구성된 現제도를 중.소기업에 맞는 맞춤형 「정보보호 안전진단」 도입 등 제도를 개선.보완

정보보호관리체계(ISMS) 인증제도 활성화

- ISMS 인증취득시 기관의 부담을 경감해주기 위하여 ISMS 인증취득 기업의 안전진단 면제기간(1년→3년) 확대 추진
- ISMS 인증취득의 자발적 참여 확대를 위하여 국가기관 또는 공기업 등의 입찰시 ISMS 인정취득 기업에 인센티브 부여 추진

Ⅳ. 기업 정보보호 수준제고 방안 – 신규제도 추진

기존제도 강화

신규제도 추진

투자환경 조성

기업의 정보보호책임자(CISO) 제도 도입

- 일정규모 이상 기업의 경우 주요 정보보호에 관한 의사결정을 하는 정보보호책임자(CISO)를 지정

공신력 있는 정보보호수준평가 필요

- (기업) 정보보안은 기업의 비즈니스 연속성을 결정하는 중요 요소로서 객관적인 정보보호 수준 공개를 통한 이미지 제고
- (이용자) 정보보호수준 확인에 따른 객관적 안전·신뢰성 확보
- (정부) 기업의 정보보호수준을 계량적으로 정확히 측정하고 이에 대한 평가를 통해 신규정책 개발 및 기존정책 보완 가능

Ⅳ. 기업 정보보호 수준제고 방안 – 투자환경 조성

기존제도 강화

기업 정보보호 투자에 대한 인센티브 제공

- 정보보호 투자금액에 대한 소득 법인세 공제율 지속 지원 예정
- 기업의 투자확대를 위하여 신규 및 복합 보안제품 및 서비스 (컨설팅 비용)에 대해서도 적용받을 수 있도록 범위 확대 추진

신규제도 추진

정보보호 취약계층에 대한 지속적 지원

- 고객정보를 취급 및 관리하고 있으나, 수행에 어려움을 겪고 있는 업체를 대상으로 취약점 점검 및 기술지원 확대 추진

투자환경 조성

정보보안 전문 인력 채용장려 추진

- 기업의 규모에 따라 일정한 정보보호 전문 인력채용을 독려하고 자체 정보보호 체계를 구축하도록 추진

V. 결론: 정보보호 제고를 위한 조치 사항

정보보호관리책임자(CISO) 도입 및 활성화 추진

- 일정규모 이상 기업의 경우 정보보호관리책임자를 지정
- 정보보호 투자계획을 정기적으로 이사회 보고 및 조치토록 제도화

기업의 모니터링 체계 구축 · 운영

- DDoS 공격과 같은 사이버테러를 탐지할 수 있도록 하는 모니터링 체계 구축 및 운영 필요
- 인터넷 침해사고 조기탐지 및 신속한 대응

정보유출 방지를 위한 내부통제 시스템 강화

- 개인정보나 영업기밀 유출시 신뢰도 하락 등으로 대규모 경제적 손실 예상
  - DDoS 공격과 같은 사이버테러에 대비한 최소한의 시스템을 구축·운영
  - 고객의 손해에 대한 피해보상을 위하여 보험가입 등 재원 확보

정보보호 예산 및 전문인력 확보 강화

- 최소한 연 평균 5% 내외의 정보보호 예산편성과 전산실 인력 중 10% 정도 할당

감사합니다.