인터넷 정보보호 종합대책

2008. 7. 22

방 송 통 신 위 원 회

목 차

1. 배경 및 현황

□ 최근 새로운 유형의 침해사고 발생, 인터넷상 대규모 개인정보 유출 및 유해정보 유포 등 인터넷 역기능 증가에 따라 종합대책을 마련

< 최근 인터넷 역기능 사례 >

침해사고 발생	o 국내 증권사 홈페이지가 분산서비스거부공격(DDoS)으로 장애 발생(3/22) o 무선랜 해킹을 통한 금융기관 정보 유출 시도 (5/11)
개인정보 유출	o 옥션에 대한 해킹으로 개인정보가 1,081만건 이상 유출(2/6) o 제2금융권, 공공기관, 요식업체 등 247개 기관 해킹으로 970만 여건 고객정보 유출(5/28)
유해정보 유포	o 초등학교 집단 성폭행 사건 발생(4/21) : 유해사이트 등이 주요 원인으로 지목 o 무선인터넷 스팸으로 인한 부당과금 관련 신고 급증(2만건/일평균)

□ '03년 1·25 인터넷 침해사고 이후 365일/24시간 인터넷 모니터링 체계를 구축하고 인터넷 정보보호에 노력하여 가시적인 성과를 달성

o '04년 이후 지속적인 침해사고 예방 및 대응으로 **웜·바이러스 피해신고**('04년 107,994건 → '07년 5,996건), 및 **해킹신고**('04년 24,297건 → '07년 21,732건) **감소**

※ 1.25 당시 전세계 피해 대비 국내 피해 비율이 약 12% 수준이었으나, 현재 2.5% 수준 → 6조 7천억의 효과 (Computer Economics 자료를 바탕으로 한국정보보호진흥원 산출)

□ 과거 해킹이 자기 과시나 네트워크 마비가 목적이었다면, 최근에는 **개인정보 탈취나 금품 갈취 등 범죄형 해킹이 증가**하는 추세

※ '07년 개인정보 탈취 등을 목적으로 하는 해킹시도(4,316건)가 전년대비 16.3% 증가

□ **불법·불건전 유해정보가 크게 확산**되는 추세이며, 이메일 스팸 수신량은 감소하여 왔으나, 휴대전화 스팸은 최근 다시 증가

※ 유해정보 시정 요구건수는 '05년 42,643건에서 '07년 112,220건으로 263.2% 증가
※ 1인당 하루 이메일 스팸수신량은 '03년 29.1통→'06년 5.3통 → '07년 4.3통
※ 1인당 하루 휴대전화 스팸수신량은 '04년 1.7통→'06년 0.47통 → '07년 0.57통

□ 우리나라가 IT인프라 구축의 선도국가임에도, 인터넷 활용을 위한 신뢰기반 미비로 세계적인 인터넷 기업 배출에는 한계가 있다는 평가

※ 아마존, 구글, 위키피디아 등 미국 기업들이 세계 인터넷 트랜드를 선도

2. 문제점

□ 기업과 정부의 정보보호 투자 미흡

o 기업의 정보보호 투자 및 인력이 낮은 수준

※ 기업의 50.8%가 보안투자 全無, 정보보호 전담직원수가 평균 100명당 0.38명

o 정부도 정보보호 예산배정에 소극적임

※ 우리나라의 정보화 대비 정보보호 예산이 4.3%(1,478억, '08년)로 미국의 1/2 수준

□ 과도한 개인정보 수집에 비해 책임의식 미흡

o 대다수 사업자들이 주민등록번호 등 서비스 제공과 무관한 개인정보를 관행적으로 수집·보관

※ 국내 개인정보 수집 웹사이트 중 62.2%가 주민번호 수집

o 다수 사업자는 개인정보 유출 사고 발생시 이미지 손상 등을 이유로 즉각적인 대처에 미온적이며, 피해구제를 위한 사후조치 등도 미진

□ 유해정보 유포 및 확산경로가 다양화·지능화

o 인터넷게시판, 휴대폰 메시지 등 다양한 매체를 통한 유해정보 확산

o 스팸 발송기법의 지능화(원링 등)·기업화 경향

※ 원링(One-ring): 한번 울리고 끊겨 발신번호로 회신을 유도하는 휴대폰 스팸

□ 인터넷 활성화에 비해 **해외발 해킹 등 침해사고 대비 취약**

o 온라인 게임 아이템을 사고 파는 문화적 특성, 마케팅을 위한 주민번호 수요가 많고, 시스템이 취약한 우리나라를 노린 해외발 해킹 증가

※ 해외로부터의 해킹시도 중 중국발이 전체의 33%~53% 차지(KISA)

※ 중국 해커들이 이용하는 해킹 툴이 1,000개가 넘는 등 중국 해킹기술이 발전하고 있으며, 한국과 문화적 동질성이 있는 중국발 해킹이 증가

o 이용자들은 정보보호의 중요성에는 공감하고 있으나, 최신 보안패치 업데이트 등 정보보호 실천으로 생활화되지는 못하는 실정

※ 인터넷 이용자 중 74.1%가 한달 1회 이하의 빈도로 보안패치 업데이트 실시

3. 목표 및 전략

□ 목 표

o 인터넷 이용환경의 안전성 제고 및 인터넷 경제의 신뢰기반 조성

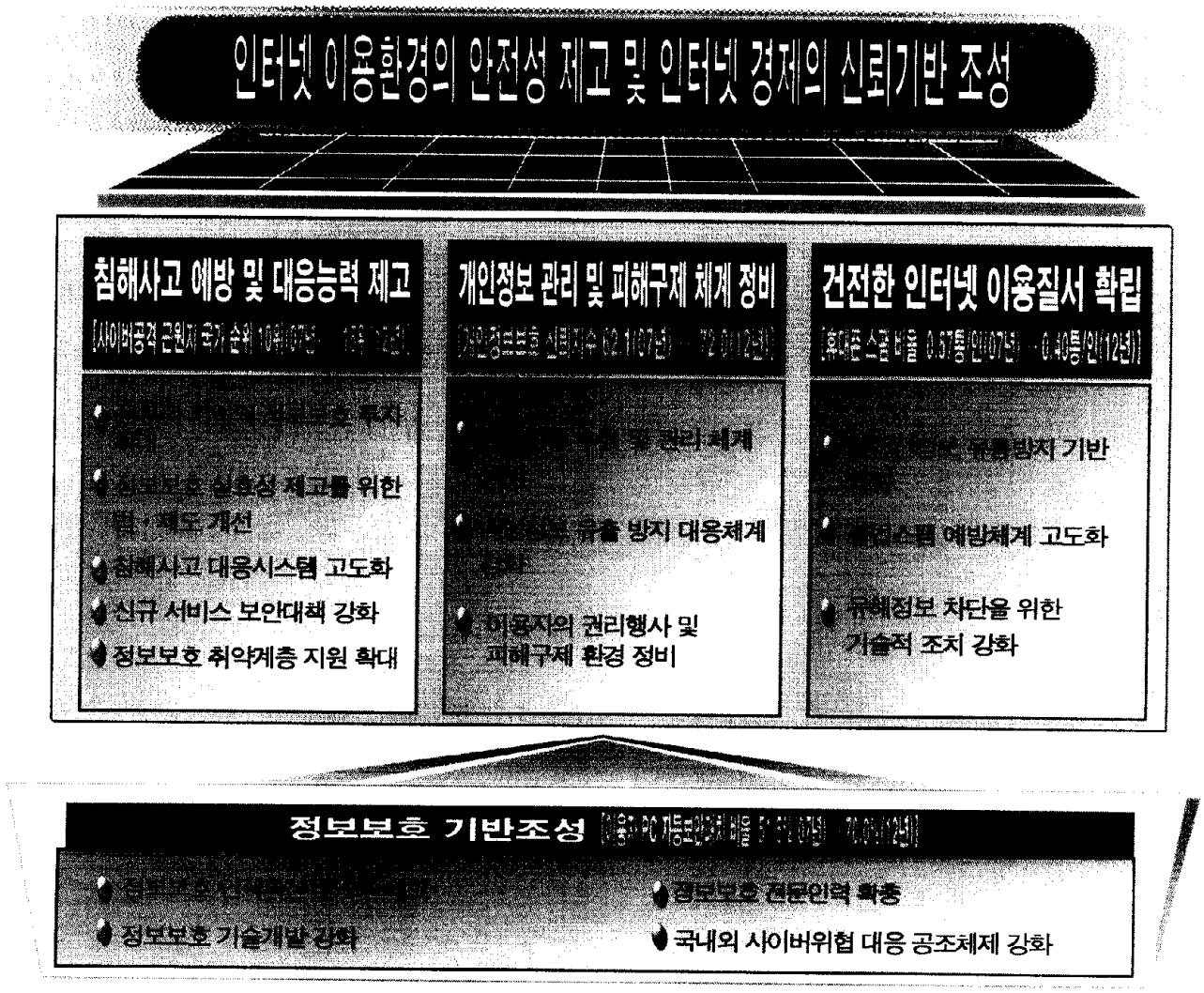
□ 전 략

o 침해사고 예방 및 대응능력 제고

o 개인정보 관리 및 피해구제 체계 정비

o 건전한 인터넷 이용질서 확립

o 정보보호 기반조성



4. 주요 대책

1 침해사고 예방 및 대응능력 제고

◆ 사이버공격 근원지 국가순위 개선 ('07년 10위 → '09년 12위 → '12년 15위)
※ 보안전문업체인 시만텍에서 매년 반기별로 180개국 이상을 대상으로 조사·발표하는 사이버 공격 근원지 국가순위에서 우리나라는 '04년 4위에서 '07년 10위로 개선

정부와 기업의 정보보호 투자 확대

□ **정부 정보보호 예산 확대**

o 국가·공공기관의 **정보화 예산대비 정보보호예산**을 '12년까지 선진국 수준으로 **확대**(기획재정부, 행정안전부 등과 협의)

□ **기업 정보보호 투자에 대한 인센티브 제공**

o 정보보호시스템 설비 투자 금액에 대한 조세감면 수혜대상 기업의 범위 및 공제율 확대 추진(기획재정부 등과 협의)

※ 현재 중소기업의 정보보호시스템 설비 투자금액의 3% 세액공제(조세특례제한법 5조)

정보보호 실효성 제고를 위한 법·제도 개선

□ **기업 CSO 제도 도입**

o 일정규모 이상의 기업에는 주요 정보보호 관련 의사결정을 하는 **정보보호최고책임자(CSO)를 두도록 의무화**

- 특히, CSO가 투자계획을 정기적으로 이사회(CEO)에 보고하도록 제도화하고, 신용평가회사가 이를 기업평가에 활용토록 유도

※ CSO(Chief Security Officer): 기업의 개인정보 관리뿐만 아니라, 해킹 방지대책 및 법률적 대응까지 총괄하는 임원

□ **정보보호 안전진단 제도 개선**

o 안전진단 수행기관의 자격요건 미준수시 인정 취소·시정 명령권 신설, 안전진단대상자에 대한 기술교육 등 안전진단 제도의 실효성 제고

□ 정보보호관리체계(ISMS) 인증제도 활성화

o 정보보호관리체계 인증업체의 국가조달 참여시 가산점 부여, 배상책임보험 가입시 할인혜택 확대 등 ISMS 제도 활성화(조달청과 협의)

□ 악성코드 삭제 및 시스템 접근 요청권 제도 도입

o 이용자에게 악성코드를 유포하고 있는 웹사이트(업체)에 대해 삭제 조치를 요청할 수 있는 **악성코드 삭제 요청권 제도 도입**

o 침해사고 발생시 신속한 초동 대응이 필요한 경우 관련 시스템을 점검할 수 있는 **시스템 접근 요청권**을 신설

※ 방통위의 시스템 접근 요청을 받은 기관은 특별한 이유가 없는 한 허용

침해사고 대응시스템 고도화

□ 「DDoS 탐지·제거시스템」 구축·운영

o DDoS 공격 대응 강화를 위해 국내 주요 정보통신서비스제공자의 연동망 구간에 DDoS 탐지·제거시스템 구축·운영

※ 분산서비스거부(DDoS : Distributed Denial of Service) : 특정서버에 대규모 유해 트래픽을 일시에 유입시켜 서비스를 마비시키는 행위

□ 「악성코드 탐지시스템」 운영 확대

o 홈페이지상 악성코드 탐지 시스템의 일일점검 사이트수 확대

□ 「웹 사이트 보안수준 확인 시스템」 구축·운영

o 이용자가 무료 소프트웨어를 PC에 설치하면, 사이트에 접속할 때마다 「웹 사이트 보안수준 확인 시스템」과 연동되어 보안서버 구축여부 등 해당 사이트의 보안수준을 자동으로 표시

신규서비스 보안대책 강화

□ 신규서비스 정보보호 사전진단 지원

o u-City 서비스 등 신규 서비스 개발시 보안취약점을 사전에 점검하여 이용자가 안심하고 이용할 수 있는 신규 서비스 시장 환경 조성

□ **신규서비스 침해사고 시험환경 구축·운용**

o IPTV, 스마트폰 등 침해사고 시험환경 구축·운용을 통한 대응기술 확보

□ **신규서비스 침해사고 모니터링 및 대응체계 구축**

o IPTV, VoIP 등 신규서비스 트래픽 정보에 대한 **모니터링 시스템을 구축**하고, **이상징후 발견시 즉시 대응**

정보보호 취약계층 지원 확대

□ **영세 중소기업에 대한 기술적 지원 강화**

o 중소기업 대상 무료 웹방화벽 보급 및 웹서버 원격점검 등 지원 확대

□ **일반 이용자 대상 침해사고 상담지원 강화**

o 118 전화상담/PC원격 점검을 위한 인력 및 시스템 확대 구축을 통해 일반 이용자 대상 침해사고 상담 및 기술 지원 강화

□ **사회 소외 계층에 정보보호 서비스 제공**

o 백신업체 등과 공동으로 장애우에게 백신보급 등 정보보호 지원

2 개인정보 관리 및 피해구제 체계 정비

◆ 개인정보보호 신뢰지수 개선 ('07년 62.1 → '09년 65.9 → '12년 72.0)

※ 기업 및 이용자의 개인정보보호 수준을 종합적으로 평가할 수 있는 지수로서 '07년 처음 개발. 개인정보취급방침 고지율, 보호조직 구성율, 암호화 저장률 등 12개 세부지표로 구성

개인정보 수집 및 관리 체계 정비

□ **인터넷상 개인정보 수집 최소화**

o **주민등록번호** 등 개인 식별번호는 전자상거래 등을 위해 **법령**으로 규정한 경우 외에는 **수집·저장·유통** 등 **처리 금지**

※ 부가가치세법 등 **주민번호 수집·보관을 의무화**하고 있는 **법령** 재검토·개정추진

o 인터넷 서비스 제공에 반드시 **필요**한 **최소한**의 **개인정보 항목** 가이드라인을 제정하여 사업자의 적절한 수집 **기준 제시**

□ **주민등록번호 대체수단 이용 활성화**

o **주민등록번호 미사용 회원가입방법** 보급을 확대하고, **아이핀**과 **G-PIN**(공공)을 **연계**하여 이용자의 사용편의성을 제고

※ 주민등록번호 미사용 회원가입방법 : 휴대폰인증, 공인인증서, 아이핀 등

□ **기 과다수집·저장 개인정보의 삭제 추진**

o 이용자가 인터넷사이트 **장기 미사용 계정**을 손쉽게 확인·탈퇴할 수 있도록 **온라인 지원 시스템** 구축·운영

o 주요 포털 등과 **장기 미사용 계정 정리캠페인**을 공동 추진

□ **방송사업자의 개인정보보호 관리수준 제고**

o **유선·위성·IPTV사업자** 등 방송사업자를 **정보통신망법 적용 대상**에 포함시켜 **개인정보보호 의무**를 **부과**

개인정보 유출 방지 대응체계 강화

□ **개인정보 유·노출 탐지시스템 구축**

o 인터넷상에서 대량 **개인정보**의 **유·노출**을 신속하게 **탐지·조치**할 수 있는 **능동적 대응체계**(일명 e-WatchDog) 구축·운영

※ 웹사이트의 개인정보 유·노출 탐지(1단계)와 포털사업자와 시스템 연동을 통한 공조체계 구축(2단계) 등 단계별로 구축

□ **개인정보 보관·전송시의 유출에 대한 피해 예방조치**

o 유출시에도 추가적인 활용이 불가능하도록 계좌번호 등 **중요 개인정보**는 의무적으로 **암호화**하여 **저장**

o 인터넷 **전송구간**에서 개인정보를 **암호화**해주는 **보안서버** 보급 확대

※ 보안서버 보급 : '09년 33,000대 → '13년 100,000대(선진국수준, 민간부문)

□ **개인정보 유·노출 사이트 접속 차단제 실시**

o 개인정보 대량 유·노출사이트가 운영자 **소재 불명, 연락두절** 등으로 **삭제 곤란시**, 피해확산 방지를 위해 **긴급 접속차단**

※ 정보통신망법 개정을 통해 ISP 등이 접속차단조치를 실시할 수 있는 근거마련

□ **개인정보보호 인증제도 도입**

o 통신·인터넷사업자의 **개인정보 수집·저장·이용·관리 체계** 전반을 점검하여 적정 수준에 도달한 사업자에 **인증 부여**

이용자의 권리행사 및 피해구제 환경 정비

□ **개인정보 유출 사실 통지제 도입**

o 개인정보 유출 등 침해에 따른 **후속피해 방지**를 위해 유출발생 사업자가 **침해 원인·내용** 등을 이용자에게 **통지**하도록 **의무화**

※ 통지 기준·절차, 통지의무 이행사업자에 대한 책임경감 등을 정통망법 개정시 반영

□ **이용자의 개인정보자기통제권 실질화**

o 회원가입시 수집·이용, 제3자 제공, 취급위탁 등을 **포괄 동의** 받는 **관행**을 **금지**하고, 각 단계별 **별도 동의절차**를 엄격히 준수

o 개인정보 제3자 제공시 "제공되는 제3자" 등의 **개별 선택·동의권** 보장

□ **개인정보침해 예방기능 및 피해구제 체계 개편**

o 민원 및 침해신고 사례의 **분석 능력**을 **고도화**하고, 사전 인지·예상되는 **침해사례**에 대해 **선제적·예방적 실태조사** 실시

※ 과징금 신설 등 제재수단 강화를 골자로 한 정통망법 시행('08.12)에 대비하여 개인정보보호 **상시점검 기능 강화 및 조직 역량 확대**

o 침해신고 민원**처리기간 단축** 등 고객만족도를 제고하고, 민원처리와 실태점검을 유기적으로 연계하여 **동종 사례 재발·확산 방지**

3 건전한 인터넷 이용질서 확립

◆ 휴대폰 스팸수신량 감소 ('07년 0.57통 → '09년 0.45통 → '12년 0.40통)
※ 인터넷전화·무선인터넷망 개방 등으로 인해 발송수법이 다양화됨에 따라, 휴대폰 스팸의 양상이 점차 악성화·기업화되고 있어 이용자 피해가 심각

불건전정보 유통방지 기반 강화

□ **포털 등의 사회적 책임강화를 위한 법·제도 개선**

o 포털, P2P 사업자 등에게 모니터링 의무를 부과하고 위반시 처벌 규정 신설

o 명예훼손 등의 피해자가 정보삭제 요청시 임시조치 등을 취하지 않는 사업자 등에 대한 처벌규정 도입

□ **익명성에 의한 인터넷 역기능 최소화**

o 악성댓글 등 익명성을 이용한 인터넷 역기능을 예방하기 위한 「제한적 본인확인제」 등 개선방안 추진

□ **포털 및 P2P 사업자 등의 불법정보 관리실태 점검 강화**

o 사업자 자율 유해정보신고센터 운영, 음란물 차단시스템 도입 여부 등 불법정보 관리실태 점검 강화

※ 「P2P 사업자 가이드라인」 등 준수여부를 점검하여 자율정화 노력 유도

불법스팸 예방 체계 고도화

□ **광고 사전수신동의(Opt-in) 예외 축소**

o 전화·팩스 광고시 사전수신동의 예외규정의 악용을 방지하기 위하여 정보통신망법 및 스팸방지 가이드라인 개정 추진

※ 통신판매업자를 예외 대상에서 제외하고, 기존 거래관계의 인정기간 축소

□ **통신사간 정보공유를 통한 악성스패머 재가입 제한**

o 스팸전송 이력이 있는 악성스패머 정보를 통신사간 공유함으로써 반복적인 서비스 재가입을 통한 스팸발송을 원천적으로 제한

□ **불법스팸 광고주에 대한 형사처벌 확대 · 강화**

o 전송자뿐만 아니라 광고주에 대해서도 형사처벌이 가능하도록 법적근거를 마련하고, '특별사법경찰권'에 따른 현장조사 강화

유해정보 차단을 위한 기술적 조치 강화

□ **통신사별 음성(전화) 스팸 탐지시스템 구축 · 운영 확대**

o 이동통신사별로 음성스팸을 조기에 탐지하고 발송 제한을 할 수 있는 시스템 구축 유도

□ **이메일 스팸 차단기술 보급 확대**

o 이메일의 IP주소를 스팸 주소목록과 대조하여 손쉽게 스팸 여부를 확인하여 차단할 수 있는 기술을 확대 보급

□ **해외 불법사이트 대상 URL 차단방식 도입**

o 국내 단속을 피해 해외에서 서비스하는 불법 음란물사이트 등을 국내에서 접속 자체가 불가능하도록 사이트 주소를 차단

□ **「아 · 태지역 실시간 스팸정보 공유시스템」 구축**

o 아 · 태지역 주요 국가간 스팸정보를 실시간으로 공유하기 위한 「AP-RBL(Asia-Pacific Real-time Blocking List) 시스템」 구축

4 정보보호 기반조성

◆ 이용자 PC 자동보안패치 비율 개선 ('07년 51.5% → '09년 55% → '12년 70%)

※ 보안이 취약한 PC는 해킹 및 웜 · 바이러스 등에 취약하고, 악성코드 유포 · DDoS 공격 · 스팸 발송 등 각종 사이버 범죄의 근거지로 악용될 수 있음

정보보호 인식확산 및 수준제고

□ **범국민 정보보호 인식제고 캠페인**

o 보안패치 업데이트 홍보, 휴면계정 정리, 스팸 대응방안 안내 등 이용자 보안의식 제고를 위한 **대규모 정보보호 캠페인 전개**

※ 포털, ISP 등과 공조하여 다양한 교육 · 홍보, 캠페인 및 콘텐츠 제공

□ **이용자 친화적이고 자율적인 정보보호 활동 강화**

o 방송매체를 통한 공익광고 방영, 정보보호 홍보대사 임명, '정보보호 기상예보', 윤리강령 · 자율규약 제정

o 초중고 대상 사이버 청정학교 선정, 정보보호 교육 실시(교과부와 협조)

정보보호 전문인력 확충

□ **해킹방어 능력을 갖춘 정보보호 전문인력 공급 지원**

o 정보보호전문가(SIS) 자격시험에서 실기시험을 강화하고, 개인정보보호책임자 자격요건에 SIS를 포함하는 등 전문가 자격제도 내실화

o 우수 정보보호 인력이 군 정보보호 병과 혹은 정보보호 전문기관에서 군 복무를 수행할 수 있도록 제도 개선(국방부와 협조)

□ **정보보호 전문인력 양성 지원**

o 해킹방어 기술을 상시 훈련할 수 있도록 온라인 훈련장 운영 확대, 대학 정보보호 동아리 지원 및 해킹방어 대회 수상자에 대한 혜택 확대

정보보호 기술개발 강화

□ **해킹 방어 기술개발**

o 해킹공격을 능동적으로 탐지하고 실시간으로 관제하는 기술 개발

□ **개인정보보호 기술개발**

o 자신의 정보를 통합적으로 관리할 수 있는 전자ID지갑 시스템 등 개인정보보호 기술개발 예산 배정 확대

국내외 사이버 위협 대응 공조체제 고도화

□ **국내 유관기관 공조 강화**

o 방통위, KISA, 포털 · 통신사업자 등 **유관기관 간 Hot-Line**을 구성하여 침해 사고 발생시 즉각적인 경보 및 신속한 대응 체계화

□ **국제 공조 강화를 위한 협력활동 강화**

o 해외발 해킹, 개인정보 불법거래, 스팸 등에 대응하기 위하여 관련 국가 및 OECD 등 국제기구와 협력활동 강화

5. 기대효과

국가정보보호 수준 제고

- 인프라, 기술, 제도 등 국가 전반의 정보보호 수준 제고
- IT강국에 걸맞는 국제적인 정보보호 위상 확보

	2007년		2012년
국가정보보호 지수	63.4점	→	80.0점
보안서버 보급률	49위	→	5위
국가 사이버 공격 근원지	10위	→	15위

☞ 국가정보보호지수 : 정보보호 수준을 계량적으로 측정·분석하기 위해 KISA에서 개발한 지표로 백신보급률, 방화벽보급률, 정보보호 예산 비율, 해킹 신고비율, 개인정보 침해신고 비율, 스팸수신 비율 등으로 구성

이용자보호 수준 제고

해킹 방지, 개인정보의 유출 및 유해정보 유통 등을 인터넷 이용자가 체감할 수 있는 수준까지 개선

	2007년		2012년
악성코드 재감염률	39.3%	→	25%
주민등록번호 수집률	62.2%	→	30%
휴대폰 스팸 수신량 감소	0.57통	→	0.40통

경제적 효과 달성

인터넷 침해사고 대응을 통한 경제적 효과 달성

	2007년		2012년
전세계 침해사고 피해액 대비 국내 피해액 비율	2.5%	→	2.0%

☞ 전세계 침해사고 피해액 대비 국내 피해액 비율은 '03년 12% 수준에서 현재 2.5% 수준으로 향후 5년간 단계적으로 2% 이하로 진입할 경우 '08년~'12년까지의 경제적인 효과는 6조원 이상으로 예상

【붙임 1】

「인터넷 정보보호 종합대책」 50개 과제 추진일정

전략	세부 추진과제	'08년	'09년	'10년	비고
침해사고 예방 및 대응능력 제고	① 정부 정보보호 예산 확대	부처 협력	예산확보	→	부처 협력
	② 기업 정보보호 투자에 대한 인센티브 제공	제도 개선	→	→	부처 협력 타법 개정
	③ 기업 CSO 제도 도입	연구반 운영	CPO 개편	CSO 도입	망법 개정 부처 협력
	④ 시스템 접근요청권 제도 도입	제도 도입	→	→	망법 개정
	⑤ 악성코드 삭제 요청권 제도 도입	제도 도입	→	→	망법 개정
	⑥ 정보보호 안전진단 제도 개선	제도 개선	사후 관리	→	망법 개정
	⑦ 정보보호관리체계(ISMS) 인증 활성화	제도 개선	심사원 양성	심사원 교육	망법 개정
	⑧ DDoS 대응시스템 구축 · 운영	3개사 구축	4개사 구축	→	기술 대책
	⑨ 악성 봇 DNS 싱크홀 적용대상 확대	대학 적용	기능개선	적용대상 확대	기술 대책
	⑩ 악성코드 분석 및 종합관리 체계 강화	시스템 점검	시스템 구축	시스템 개선	기술 대책
	⑪ MC-Finder(악성코드 탐지시스템)	점검대상 확대	→	→	기술 대책
	⑫ 웹쉘 탐지	시스템 개발	시스템 적용	→	기술 대책
	⑬ 웹사이트 보안수준 확인시스템 시범구축 · 운영	시스템 구축	시범 운영	민간 이양	기술 대책
	⑭ 초고속 인터넷 이용자를 위한 정보보호 S/W 보급 확대	법적 근거 마련	보급 캠페인	→	망법 개정 기술 대책
	⑮ 신규 서비스 정보보호 사전진단 지원	시범 적용	SLA 마련	제도화	기 타
	⑯ VoIP 대책	연구반 운영	관제시스템 개발	대응체계 구축	기술 대책
	⑰ IPTV 대책	연구반 운영	관제시스템 개발	대응체계 구축	기술 대책
	⑱ 무선환경 대책	연구반 운영	대책 마련	대응체계 구축	기술 대책
	⑲ 무료 웹방화벽 보급 확대	웹방화벽 보급	지원반 운영	보급 확대	기술 대책
	⑳ 웹취약점 점검	웹취약점 점검	시스템 구축	서비스 확대	기술 대책
	㉑ 일반 이용자 침해사고 상담지원 강화	상담지원	시스템 · 인력 확대	서비스 확대	기술 대책
	㉒ 사회 소외계층에 정보보호 서비스 제공	동아리 중심	청소년 교육	전국 확대	기 타
개인정보관리 및	㉓ 인터넷상 개인정보 수집 최소화	유형별 가이드	관련법률 개정	→	부처 협력 타법 개정
	㉔ 주민등록번호 대체수단 이용 활성화	적용의무화	홍보 및 유도	단계별 적용	부처 협력 기술 대책
	㉕ 기 과다수집 · 저장 개인정보의 삭제 추진	구축 계획	시스템 개발	운영, 안정화	기술 대책
	㉖ 방송사업자의 개인정보보호 관리 수준 제고	제도 개선	과징금 기준	방송분야 확대	망법 개정

전략	세부 추진과제	'08년	'09년	'10년	비고
피해구제체계 정비	㉗ 개인정보 유·노출 탐지시스템 구축	ISP 수행	시스템 개발	센서망 구축	기술 대책
	㉘ 개인정보 보관·전송시의 유출에 대한 피해 예방조치	보호기준 강화	솔루션 보급	기술지원 강화	기술 대책 고시 개정
	㉙ 개인정보 유·노출 사이트 접속 차단제 실시	실행계획 마련	법제화 추진	단계별 적용	망법 개정
	㉚ 개인정보보호 인증제도 도입	실행계획 마련 및 법제화	단계별 적용	망법 개정	망법 개정
	㉛ 개인정보 유출 사실 통지제 도입	법제화 추진	단계별 적용	→	망법 개정
	㉜ 이용자의 개인정보 자기 통제권 실질화	실행계획 마련 및 법제화	제3자 제공 확인시스템 권고		망법 개정
	㉝ 개인정보침해 예방기능 및 피해구제 체계 개편	체계 개편	→		기 타
건전한 인터넷 이용질서 확립	㉞ 포털 등의 사회적 책임강화를 위한 법·제도 개선	법령 개정	사업자 점검 및 처벌		망법 개정
	㉟ 익명성에 의한 인터넷 역기능 최소화	개선방안	법령 개정	적용 확대	망법 개정
	㊱ 포털 및 P2P 사업자 등의 불법정보 관리실태 점검 강화	불법정보 관리실태 및 가이드 준수여부 점검			기 타
	㊲ 광고 사전수신동의(Opt-in) 예외 축소	가이드라인 및 법령 개정	→		부처 협력 망법 개정
	㊳ 통신사간 정보공유를 통한 악성 스패머 재가입 제한	과태료 부과 관리시스템 구축	악성스패머 정보공유 시스템 구축·운영		망법 개정
	㊴ 불법스팸 광고자에 대한 형사처벌 확대·강화	법령 개정	형사처벌 대상 수사 강화		망법 개정
	㊵ 통신사별 음성(전화)스팸 탐지시스템 구축·운영 확대	구축 유도	→		기술 대책
	㊶ 이메일 스팸 차단기술 보급 확대	보급 확대	→		기술 대책
	㊷ 해외 불법 사이트 대상 URL 차단방식 도입	차단기기 설치	불법사이트 URL 접속 차단		기술 대책
	㊸ 「아·태지역 실시간 스팸정보 공유시스템(AP-RBL)」구축	시스템 개발	스팸정보 공유 및 차단 활용		기술 대책
정보보호 기반조성	㊹ 범국민 정보보호 인식제고 캠페인	프로그램 마련	캠페인 시행	→	기 타
	㊺ 이용자 친화적이고 자율적인 정보보호 활동 강화	실행계획 마련	방송매체 활용	정보제공 확대	부처 협력
	㊻ 해킹방어 능력을 갖춘 정보보호 전문인력 공급 지원	부처 협력	제도 개선	확대 실시	부처 협력
	㊼ 정보보호 전문인력 양성 지원	실행 계획	지원 실시	→	부처 협력
	㊽ 정보보호 기술개발(해킹방어, 개인정보보호)	침입대응 기술	사용자 ID 관리	N/W 보안	기술 대책
	㊾ 국내 유관기관 공조 강화	핫라인 강화	→		부처 협력
	㊿ 국제공조 강화를 위한 협력 활동 강화	실행 계획	협력과제 제안	국제협력 주도	기 타

【붙임 2】

인터넷 침해사고 예방 및 대응의 경제적 효과

o '03년 1.25 인터넷침해사고 이후 전세계 피해액 대비 국내 피해액(침해사고 대응체계 개선 전과 후)을 추정하여 경제적 효과를 산출

< 연간 침해사고 피해액 추정 >

(단위 : 억원)

연도		2003	2004	2005	2006	2007	소계	2008	2009	2010	2011	2012	소계
전세계		154,830 ($13 Billion)	200,317 ($17.5B)	145,408 ($14.2B)	127,015 ($13.3B)	127,015 ($13.3B)	754,585	127,015 ($13.3B)	127,015 ($13.3B)	127,015 ($13.3B)	127,015 ($13.3B)	127,015 ($13.3B)	635,075
국내	개선전	18,270 (11.8%)	23,637 (11.8%)	17,158 (11.8%)	14,988 (11.8%)	14,988 (11.8%)	89,041	14,988 (11.8%)	14,988 (11.8%)	14,988 (11.8%)	14,988 (11.8%)	14,988 (11.8%)	74,939
	개선후	4,800 (3.1%)	6,210 (3.1%)	4,508 (3.1%)	3,175 (2.5%)	3,175 (2.5%)	21,868	3,048 (2.4%)	2,921 (2.3%)	2,794 (2.2%)	2,667 (2.1%)	2,540 (2.0%)	13,972

※ 전세계 피해액은 미국 Computer Economics사(2006 Malware Report)가 매출손실, 생산성저하, 복구비용 등을 토대로 산출된 결과이며 '07년 이후는 '06년 피해액을 적용

※ 괄호안의 %는 전세계 피해액 대비 국내 피해액 비율

o '07년 이전의 국내 피해액 및 경제적 효과 산출

- 대응체계 개선전 피해액: '03년 CAIDA의 보고에 따르면, 전세계 감염시스템은 약 7만5천개, 국내 감염시스템은 8천8백여개로 조사되어 전세계 대비 11.8%

※ CAIDA : Cooperative Association for Internet Data Analysis

- 대응체계 개선 후의 피해액과 경제적 효과: '05년, '06년 실태조사에서 확인된 피해액('05년 4,500억원과 '06년 3,100억원)과 전세계 피해액 간의 비율을 적용하여 경제적 효과 산출

※ 경제적 효과 : 개선전 합계(89,041억원) - 개선후 합계(21,868억원) = 약 6조7천억원

o '08년~'12년의 경제적 효과 전망

- 대응체계 개선전의 전세계대비 피해액비율은 11.8%를 그대로 적용하고 개선후는 지속적인 노력에 따라 연간 0.1%씩 감소 예상

※ 경제적 효과 : 개선전 합계(74,939억원) - 개선후 합계(13,972억원) = 약 6조원

【붙임 3】

사이버 공격 근원지 국가 순위

□ 개 요

o 글로벌 보안업체인 시만텍은 6개월 단위로 전세계 인터넷 침해사고 동향을 발표하면서, 침해사고 관련한 국가 순위를 발표

※ 시만텍은 전세계 180여개 국가에 분포된 약 4만여개의 고객사 방화벽 및 침입탐지 시스템으로부터 정보 수집하고 있으며, 약 1억 2천만개 정도 사용되고 있는 시만텍 백신 프로그램으로부터 수집된 정보를 활용

□ 침해사고 관련 국가 순위

o 시만텍 보고서의 주요 분석 항목인 **사이버공격 근원지 국가** (originating country: Attack Rank) 순위에서 **한국은 10위**로 '05년 상반기 이후 **10위권 안팎을 유지**

공격근원지 국가 : 실제 해커가 존재하는 국가를 의미하는 것은 아니며, 공격이 발생한 시스템이 위치한 국가를 의미함. 즉, 중국에 거주하는 해커가 백악관 홈페이지를 공격하기 위해 한국에 위치한 시스템을 이용할 경우 한국이 공격근원지 국가가 됨
⇒ 따라서, 공격근원지 국가 순위는 보안이 취약한 시스템의 존재 정도를 나타내는 지표로 해석되기도 함

< 사이버공격 근원지 국가 순위 >

구분	1위	2위	3위	4위	5위	6위	7위	8위	9위	10위
'04 하반기	미국 30%	중국 8%	독일 8%	**한국 4%**	캐나다 4%	영국 4%	프랑스 3%	일본 3%	스페인 3%	이탈리아 2%
'05 상반기	미국 33%	독일 7%	영국 7%	중국 6%	프랑스 5%	스페인 5%	캐나다 4%	일본 4%	**한국 3%**	이탈리아 3%
'05 하반기	미국 31%	중국 7%	영국 6%	독일 5%	프랑스 4%	캐나다 4%	스페인 3%	일본 3%	이탈리아 2%	**한국 2%**
'06 상반기	미국 37%	중국 10%	독일 6%	영국 5%	프랑스 5%	캐나다 4%	스페인 3%	일본 3%	이탈리아 2%	**한국 2%**
'06 하반기	미국 33%	중국 -	독일 -	프랑스 -	캐나다 -	영국 -	스페인 -	미확인	**한국** -	이탈리아 -
'07 상반기	미국 25%	중국 -	독일 -	프랑스 -	영국 -	스페인 -	캐나다 -	이탈리아 -	미확인	일본 -
'07 하반기	미국 24%	중국 -	독일 -	스페인 -	영국 -	프랑스 -	캐나다 -	이탈리아 -	브라질 -	**한국** -

【붙임 4】

개인정보보호 신뢰지수

□ 개요

o 개인정보 보호수준을 종합적으로 파악하여 개인정보보호정책 수립을 위한 기초 자료로 활용할 필요성이 증가함에 따라

- 기업과 개인 부문별 개인정보보호 수준을 측정할 수 있는 지수를 개발

□ 지수 개발 경과

o '개인정보보호 신뢰수준 산출모형 개발에 관한 연구'(06.12.)

o 개인정보보호지수 산출을 위한 지표항목 설정('07.5.)

o '07년 설문조사 실시('07. 6~9월)

※ 설문대상 : 종사자 수 5인 이상인 2,500개 기업 및 개인 4,000명

o 기업 및 개인부문 지표항목 종합·분석(07.10~11월)

□ '07년 개인정보보호 신뢰지수 산출 결과 : 62.1

o 기업부문 개인정보보호 지수(62.0)와 개인부문 개인정보보호 지수(62.3)를 종합하여 62.1 산출

< 개인정보보호 신뢰지수 지표구성 항목 및 산출 세부결과 >

부분별 산출지수		대항목 (산출 지수)		중항목	통계 산출항목
기업	62.0	관리	68.7	개인정보보호정책(a)	○ 개인정보취급방침 고지율(a_1)
				개인정보보호 조직 · 교육(b)	○ 개인정보보호조직 구성율(b_1)
					○ 개인정보보호교육 실시율(b_2)
		기술 · 물리	55.3	보안기술(c)	○ 암호화 통신율(c_1)
					○ 암호화 저장율(c_2)
				물리적 보안 (d)	○ 물리적 접근통제율(d_1)
개인	62.3	관리	53.9	개인정보보호정책(e)	○ 개인정보보호정책 확인율(e_1)
				ID/PW관리율(f)	○ PC 및 웹사이트 비밀번호 관리율(f_1)
					○ 공인인증서 사용율(f_2)
		기술 · 물리	79.3	보안프로그램 이용율(g)	○ 악성코드 제거프로그램 사용율(g_1)
					○ 인터넷 보안 설정율(g_2)
					○ OS업데이트율(g_3)

용어해설

CSO(Chief Security Officer, 최고 정보보안 책임자)

기업에서 내부 정보 보안을 위한 대책을 책임지고 기술적 대책과 법률적 대응까지 총괄 책임을 지는 최고 임원

DDoS(Distributed Denial of Service, 분산서비스거부) 공격

동시에 대량의 유해 트래픽을 공격대상 시스템에 전송하여 해당 시스템의 정상적인 서비스를 방해하는 사이버 공격의 일종

i-PIN(Internet Personal Identification Number)

인터넷상에서 본인을 식별하기 위해 주민번호대신 사용하는 수단

VoIP(Voice over Internet Protocol)

음성 데이터를 인터넷 프로토콜 데이터 패킷으로 변화하여 일반 전화망에서의 통화를 가능하게 해주는 통신서비스

IPTV (Internet Protocol Television)

초고속 인터넷망을 이용하여 제공되는 양방향 텔레비전 서비스

원링(One-ring) 스팸

전화벨이 1~2번 울린 후 끊어 수신자가 호기심에 통화를 연결하면 녹음된 음성멘트가 나오거나 대출상담 등 유도

P2P(Peer to Peer)

인터넷에서 개인과 개인이 직접 연결되어 파일을 공유하는 방식

RBL(Real-time Blocking List)

실시간스팸차단리스트, 국내·외 스팸정보를 실시간으로 취합·분석·확인하여, 스팸차단을 위해 등급별로 제공하는 IP 리스트