미래 지식정보사회의 정보보호 전략 프레임워크

황중연
한국정보보호진흥원

요 약

우리나라는 세계 최고 수준의 IT 인프라를 기반으로 네트워크 및 서비스 융합, RFID 등 u-IT 서비스 확산 등을 통해 유비쿼터스 사회로 빠르게 진입하고 있다. 향후 디지털 융합이 가속화됨에 따라 시간과 공간의 제약 없이 원하는 정보의 획득 · 활용이 증가하고, u-Health, u-learning 등 IT가 타산업과 융합되면서 높은 부가가치를 창출할 것으로 전망된다.

그러나 정보화의 급속한 진전에 따른 사회 전반의 편의성과 효율성이 향상하였으나, 해킹 · 바이러스, 개인정보 유출 사고, 스팸 등 역기능으로 인한 피해도 확산되고 있다. 최근에는 네트워크 방어체계를 무력화시키는 지능화된 해킹, 대량의 고객정보 유출, 사회공학 기법을 활용한 피싱 등 이용자의 자산과 프라이버시를 침해하는 사이버범죄 증가 등으로 이용자 자산과 권리 보호 관점에서의 정보보호의 중요성이 부각되고 있다.

향후 시간과 장소에 상관없이 지식정보를 활용하여 편리하고 쾌적한 생활을 누리게 하는 지식정보사회는 예측 불가능한 위험이 곳곳에 산재한 정보위험사회로의 진입을 의미할 수도 있다. 그러므로 미래사회에서 예상되는 위협을 예측하여 효과적으로 사전에 예방할 수 있는 체계를 마련하는 것은 안전하고 신뢰할 수 있는 지식정보사회를 향유하기 위한 전제조건으로 작용한다.

이에 본고에서는 미래 지식정보사회에 대비한 정보보호 전략으로 안전한 u-사회 청사진 설계 및 환경조성 선도와 국제화, 사이버위협 예방 및 대응체계의 입체적 조화와 융합, 정보보호 기술 · 제품 · 산업간 선순환 촉진과 성장 등 3대 전략을 설정하고 실행방안을 제시한다.

I. 서 론

우리사회는 세계 최고 수준의 IT 인프라를 기반으로 전 국민의 사이버생활 보편화, 디지털경제로의 전환, 산업간 융복합화가 가속화되고 있다. 또한 모바일 기술의 발전, 네트워크 컨버전스 등을 통해 유비쿼터스 사회로의 변화를 맞이하고 있다.

현재 우리나라의 정보화는 선진 일류국가 수준으로 진입하였으며, 특히 ITU의 디지털기회지수 세계 1위, UN의 전자정부 2~5위 등 세계 선도국가로 평가받고 있다.

반면, 정보화 의존도가 높아지면서 사이버상의 사회적 · 경제적 위험도가 증가하고 있으며, 최근 대량의 개인정보 유출 사고가 빈번히 발생하여 사이버거래에 대한 불안이 확산되고, 경제적인 피해도 증가하고 있다. 광대역통합망(BcN) 등 첨단인프라를 기반으로 다양한 방통융합 서비스가 제공되는 환경에서는 사이버공격으로 인한 인터넷망에서의 피해가 방송망, 통신망 등으로 확산될 위험이 매우 커지고 있다.

최근 분석에 따르면, 우리나라에서 인터넷 침해사고로 인한 경제적 손실은 연간 약 4,500억원에 이르는 것으로 나타난 바 있으며, 내부직원의 고객정보 유출, 사업자의 개인정보 무단이용 및 관리 부주의, 해킹 등 외부 공격 등으로 인한

개인정보 유출피해 규모도 심각한 수준에 이르고 있다. 또한 무차별적으로 살포되는 악성스팸으로 인한 사회경제적 손실도 지속적으로 발생하고 있다. 더불어 비윤리적 · 반사회적 내용의 콘텐츠들이 개방된 네트워크를 통해 급속히 전파되면서 사이버공간을 오염시키고 있다.

이와 같이 시간과 장소에 상관없이 편리하게 정보를 활용하는 지식정보사회로의 진입은 동시에 예측 불가능한 위험이 곳곳에 산재한 '정보위험사회'로의 진입을 의미하고 있다. 즉 고도화되고 복잡해진 정보기술이 사회시스템의 핵심 기반으로 이용되고 디지털 컨버전스가 확대되면서 특정 기술의 약한 고리에서 발생한 위험이 도미노 현상을 일으켜 전 사회의 위기로 몰아 갈 수 있는 잠재적 가능성이 상존하게 된다.

이에 따라 선진 각국에서는 정보보호 관련 국가적 차원에서의 대응전략을 마련하고, 예산 및 제도 기반을 확충하고 있다. 미국의 경우 국토안보부(DHS) 신설과 더불어 사이버 침해대응, 인식제고 등을 위한 '국가 사이버공간 보호전략'을 수립하여 추진하고 있으며, EU는 네트워크 및 정보보호 기구(ENISA)를 중심으로 인터넷 안전 및 이용자 보호를 위한 'Safer Internet Plus' 프로젝트를 추진하고 있다. 일본은 내각관방 소속 정보보호센터와 IT 전략본부 소속 정보보호 정책회의를 신설하여 국가차원의 '정보보호 기본계획'을 수립하여 추진하고 있다.

우리 정부는 2008년 새롭게 부상하는 사이버 도전과 신규 위협에 대응하고, 안전하고 신뢰받는 지식정보사회를 구현하기 위해 국가차원의 '정보보호 중기 종합계획'을 마련하였다.

이와 더불어 인터넷상의 새로운 유형의 침해사고 및 대규모 개인정보 유출 및 유해정보 유포를 방지하기 위해 인터넷 정보보호 종합대책'을 마련하여 추진하고 있다.

미래사회에서 예상되는 위협을 예측하여 효과적으로 사전에 예방할 수 있는 체계를 마련하는 것은 안전한 신뢰할 수 있는 지식정보사회를 향후하기 위한 전제조건으로 작용한다. 이에 본고에서는 미래 지식정보사회에 대비한 정보보호 추진전략과 구체적인 실행방안을 제시한다.

II. 정보보호 전략설정을 위한 기본원칙

첫째, 모든 정보보호 주체의 참여와 협력을 기반으로 정책을 추진한다. 이를 위해 정부, 공공기관, 민간기업, 개인 등 모든 정보주체가 자율적이고 적극적인 참여를 통해 정책을 수립하고, 사이버침해 공동대응, 정보보호 인식제고, 인력양성, 기술개발 등 국가 전반의 정보보호 수준제고를 위해 산학연관 협력을 강화한다. 아울러 정부는 국가안보 및 경제안정에 파급효과가 높은 사이버정보를 수집 · 분석 · 공유하여 민간부문에 제공함으로써 민간부문의 정보보호를 촉진한다.

둘째, 국민의 안전과 권리를 최대한 보장하는 방향으로 정보보호 정책을 추진한다. 이를 위해 국민 권익 보장을 위해 정보보호 정책형성, 정책집행, 정책평가 전 단계에서 이해관계자와의 협의 체계를 강화하며, 보안과 프라이버시가 상호보완적으로 작용할 수 있도록 정책의 투명성을 제고한다.

셋째, 정부 규제 중심에서 기업의 자율규제 중심으로 전환하여 정보보호 산업 수요를 촉진할 수 있도록 정책을 추진한다. 이를 위해 직접적인 기업 규제를 완화하고, 정보주체가 자율적으로 자산을 보호할 수 있는 문화를 조성한다. 또한 개인 및 기업의 정보보호 인식 제고를 통해 정보보호 제품에 대한 신규 수요를 창출하고, 신기술 활용 및 일자리 창출 등 정보보호 선순환 체계를 조성한다.

넷째, 정보보호 정책의 비용효과를 높이기 위해 정책의 중요성, 긴급도 등에 대한 사전 검토를 통해 정책과제의 우선순위를 결정하여 단계적으로 추진한다.

III. 정보보호 추진전략 및 실행방안

1. 안전한 u-사회 청사진 설계 및 환경조성 선도와 국제화

미래 정보사회의 위협을 사전에 예측하여 최적의 대응전략을 마련함으로써 안전하고 신뢰할 수 있는 미래 지식정보사회를 기획한다. 정부 조직 개편에 따라 분산된 정보보호 체계를 통합조정하기 위해 국가 전반의 정보보호를 총괄하는 국가 CSO (Chief Security Officer) 기능을 정립하고, 국경

을 초월한 사이버위협에 대응하기 위한 글로벌 정보보호 협력체계를 강화한다.

가. u-사회 위협 예측 및 정보보호 정책개발

신뢰할 수 있는 유비쿼터스 환경 구현을 위한 비전 설정 및 전략적 방향 설정이 중요하다. 사회시스템의 전 분야에서 IT의 활용이 증가함에 따라 정치, 경제, 사회, 문화 등 다양한 분야의 메가트랜드 분석 및 미래 사이버위협을 예측하기 위한 선행연구가 필요하다.

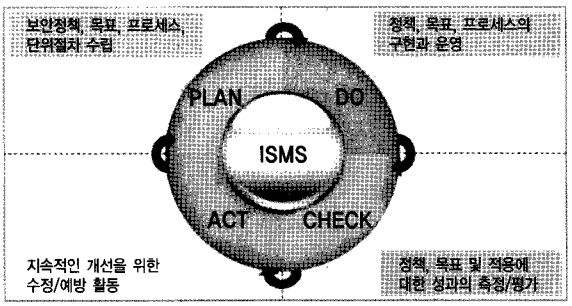
더불어 포털에서 UCC, 게시판 등을 통해 이용자들의 사이버 정치참여, 커뮤니티가 활성화됨에 따라 이용자들의 정보보호 인식을 제고하고, 자발적으로 정보보호를 실천할 수 있는 정책을 마련하여야 한다.

아울러 사이버공격으로 인한 국가사회 전반에 걸친 사이버재난 피해를 최소화하기 위해 국가 차원의 사이버위기관리를 위한 체계를 개선하고, 정부 부처별 CSO 제도 도입, CSO 협의회 운영 등을 통해 바람직한 국가 정보보호정책을 설정하여 정책간의 일관성 유지 및 정책 추진력이 요구된다.

나. 기업 유형별 정보보호 거버넌스[1] 체계 정착

최근 사회적인 문제가 되고 있는 기업의 정보자산 및 고객정보 유출 피해를 최소화하기 위해서는 기업 최고 경영층의 적극적인 참여와 지원을 통해 기업에 적합한 정보보호 관리체계를 구축하고 임직원의 자발적인 정보보호 참여가 선결되어야 한다. 이를 위해 정부의 기술적 · 관리적 지원도 요구된다. 기업 유형 및 규모에 적합한 의료 · 교육 분야 등 맞춤형 정보보호관리체계(ISMS) 모델을 개발하여 보급하고, ISP, IDC, 쇼핑몰, 포털 등 주요 정보통신서비스제공자의 중요한 정보자산 보호를 강화하기 위해 안전진단 수행기관 사후관리, 결과검토 및 개선명령 등 안전진단 제도를 변화하는 기업의 IT환경에 적합하도록 지속적으로 개선할 필요가 있다.

아울러 정보보호 대응능력이 취약한 IT 중소기업에 대한 정부 지원을 확대하여야 한다. IT 중소기업의 침해사고 예방 및 대응 능력을 향상시키기 위해 웹 취약점 점검 등 기술적 보호대책을 지원하고, 정보보호 컨설팅, 인식제고 교육 등을 강화하고, 이를 효과적으로 지원하기 위한 '중소기업 정보보호 온라인 지원센터' 구축 및 운영이 요구된다.



(그림 1) 정보보호관리체계 구성

다. 정보보호 리터러시(literacy)[2] 함양 및 문화 확산

웹해킹, 피싱 등 사회공학기법을 이용하여 침해유형이 지능화 · 다양화되는 상황에서 기술수단을 통한 침해대응만으로는 실효성에 한계가 있다. 전 국민의 기본적인 소양으로서의 정보보호 리터러시를 함양하여 생활 속에서 자율적으로 정보보호를 실천하는 문화조성이 병행되어야 한다.

구체적으로 이용자의 자율적인 실천력 향상을 위한 대규모 캠페인 전개, 방송매체를 통한 공익광고 확대, 이용자 친화적 정보보호 실천규약(윤리강령 · 자율규약 등) 제정 및 보급 등을 통해 이용자 친화적이고 자율적인 정보보호문화를 확산하여야 한다.

또한 정보보호 기상예보 등을 통해 정보보호 정책 및 실천사항 등을 상시적으로 홍보하는 것이 중요하다. 또한 공공 · 민간 분야별 · 정보보호 문화운동 협의체를 구성 및 운영하여 문화운동이 지속적이고, 실제적으로 추진될 수 있는 체계를 마련하여야 한다.

이와 병행하여 정보보호 대상별로 특화된 온 · 오프라인 연계 교육 서비스 강화가 필요하다. 기존 IT 인력에 대해서는 정보보호 최신기술 및 전환교육을 통해 기업이 필요한 인력을 적시에 제공할 수 있다. 초 · 중 · 고 교사에 대한 정

01_ 기업의 전략과 목표에 부합되도록 정보보호와 관련된 IT자원 및 프로세스를 통제, 관리하는 체계
02_ 일반인 등이 정보보호에 대한 기본적인 인식을 갖추고 있으며, 생활 속에서 실천할 수 있는 역량

보보호 교육을 강화하고, 청소년의 실천의식을 제고하기 위한 교육을 강화하여야 한다. 정보보호 관련 대학 동아리 참여자를 전문가로 양성하기 위한 고급과정을 개설하여 최신 보안기술, 평가 등 전문교육과정을 거쳐 취업과 연계하는 프로그램도 확대하여야 한다. 특별히 중소기업 종사자, 주부, 미취학 아동 등을 배려하기 위해 사이버 원격교육 프로그램을 개발하여 서비스할 필요가 있다.

이를 통해 산업체가 직접적으로 필요로 하는 기술과 직무능력을 갖춘 인재를 적시에 공급할 수 있는 기반을 마련하고, 국가경쟁력의 원천인 핵심인력을 확보함은 물론 일반인에 대한 체계적인 정보보호 문화 서비스를 확산하고, 이용자의 자율적인 실천력이 향상될 것으로 될 것으로 기대된다.

라. 글로벌 정보보호 협력체계 강화

FTA 확대 등 글로벌 경제 환경에서 인터넷을 이용하여 국경을 초월한 전자거래가 지속적으로 증가하고 있으며, 다국적 기업을 통해 국가간 정보의 유통도 빠르게 증가하고 있다. 그러나 국가간 거래의 증가와 병행하여 중국 등 해외에서 발생하는 해킹, 스팸 등 침해사고로 인해 타국이 피해를 발생하는 사례도 점증하고 있다. 이에 따라 침해사고에 대한 국제적인 공조가 절실한 상황이다.

국제적인 정보보호 협력 및 공조를 위해 정보보호정책 협력 네트워크 구축이 우선적으로 요구된다. 글로벌 정보보호 협력 및 논의를 위한 포럼을 설립하여 정책정보를 교류하고, 민간부문의 연구개발 상호협력 프로그램을 한층 강화하고, OECD, APEC, ITU 등 주요 국제기구에서의 정보보호 교류협력을 강화하여야 한다.

또한 글로벌 침해사고 대응 협력체계 강화가 필요하다. 해외 침해사고대응팀과 긴밀한 협력을 통한 국제 대응체계를 고도화하고, 악성코드 및 취약점 정보교류 및 긴급대응을 위한 글로벌 정보보호기업 협력 채널을 확대하며, 아태지역 개발도상국의 침해대응 역량강화 지원을 위한 전문교육 및 침해사고대응센터 구축 컨설팅 사업을 전개할 필요가 있다.

아울러 국제적으로 우수한 국내 정보보호 기술을 발굴하여 국제 표준화를 추진함으로써 국내 산업체의 국제적인 경쟁력을 확보할 수 있도록 적극적으로 지원해야 한다.

이러한 노력을 통해서 국제사회에서의 정보보호 리더쉽을 강화하고, 정보보호기술의 국제 경쟁력을 강화함으로써 국내 기업의 글로벌 시장 진출 확대를 도모해야 한다.

2. 사이버위협 예방 및 대응체계의 입체적 조화와 융합

미래사회의 사이버위협에 대한 효과적인 대응을 위해서는 개별적인 대응체계로는 한계가 있다. '네트워크', '소프트웨어', '개인정보', '이용환경' 등 개별적인 정보보호 대상을 서로 유기적으로 연계 및 융합하고, 침해요인과 위협에 대한 통합적 분석을 통해 다양한 정보보호대책의 상호연계성을 강화하고 종합적인 대응체계를 구축함으로써 대응활동의 시너지 효과를 극대화할 수 있다.

가. 융합네트워크 침해사고 예방 및 대응능력 강화

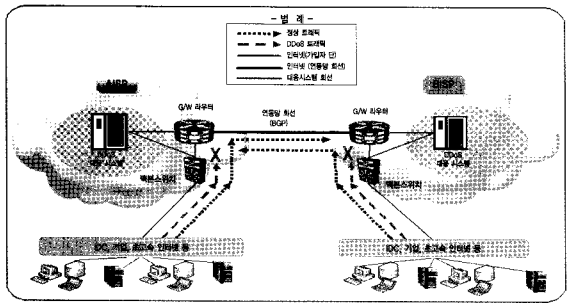
인터넷 침해사고로 인한 사회경제적 피해를 대폭 감소시키기 위해 네트워크 침해사고에 대비한 예방 및 대응체계 강화가 중요하다. 특히 BcN 등 융합네트워크에서 예상되는 위협을 사전에 예측하고, 신규 IT 기기의 취약점을 탐지하여 개선하는 예방체계를 구축하는 것이 필요하다. 구체적으로 융합네트워크 환경의 침해사고 예방 및 대응체계를 고도화하기 위해 분산서비스거부공격(DDoS[3]) 대응체계를 구축하여 운영하고, 차세대 스마트폰 및 유 · 무선 연동 융 · 복합 서비스에서의 침해사고 대응체계를 구축하고, IPTV 등 신규 융합 네트워크에서의 침해사고 대응 체계를 구축하여야 한다. 정보보호 취약계층에 대해서는 웹 취약점 원격 점검 서비스를 실시하고, 웹 방화벽을 무료로 보급하여 지원을 강화할 필요가 있다.

또한 융합네트워크 환경의 시스템 취약점을 최소화하기 위해 온라인 배포 프로그램 및 공개 S/W 안전성 점검 강화와 더불어 융합네트워크 대상 악성코드 은닉 탐지 시스템을 확대하고 악성코드 신속 대응을 위한 분석 자동화 및 종합관리 체계 구축 및 상시적 운영이 요구된다.

아울러 국내 인터넷연동망 구간에 DDoS[4] 공격을 탐지하고 차단할 수 있는 DDoS 대응시스템 구축을 확대할 필요가 있으며, 인터넷 연동망구간(IX)에 대한 정부차원의 시범구

03_ DDoS(Distributed Denial of Service) : 특정서버에 대규모 유해트래픽을 일시에 유입시켜 서비스를 마비시키는 사이버 공격

축을 통해 ISP의 DDoS 보안인식을 제고하고, 자발적인 DDoS 대응 투자를 유도할 필요가 있다.



(그림 2) DDoS 대응시스템 구성도

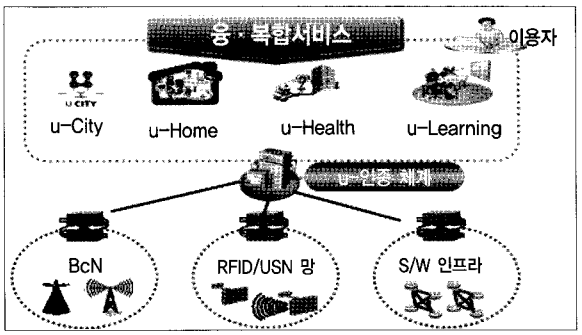
이러한 침해사고 예방 및 대응활동을 통해 악성봇 감염률을 현재 수준 대비 10% 이하로 획기적으로 감소시키고, 악성코드 은닉 재발률도 매년 10% 감소해서 인터넷의 안전성을 향상시킬 수 있을 것으로 기대된다. 또한 광대역통합망(BCN) 등 융합네트워크의 안전성과 신뢰성을 확보하여 신규 IT 서비스의 신뢰기반을 조기에 마련할 수 있을 것으로 예상된다.

나. 융 · 복합 서비스 체계의 안전 · 신뢰성 강화

현재 우리나라의 공인인증서비스 이용자 수는 1,600만 명에 이르러 온라인상의 안전한 거래를 위한 기반은 마련되어 있다고 할 수 있다. 그러나 메모리 해킹 등 해킹 기술 발전으로 인한 인증서 유출 우려가 증가되고 있으며, IPTV, VoIP, 무선랜 해킹 등 무선 인터넷 및 방통융합 서비스 활성화와 더불어 신규 위협이 발생할 것으로 예상됨에 따라 이에 대한 대응체계 구축이 긴요하다.

신규 IT 서비스의 안전 · 신뢰성을 확보하기 위해 서비스별 인증 기준 등을 정의한 통합전자인증 프레임워크를 개발하여 보급하고, 전자태그 등 다양한 기기에 대한 전자인증 서비스 제공을 위한 제도 및 기술을 확보할 필요가 있다. 통합전자인증체계에서는 인증수단이 PKI기반에서 바이오정보, 전자태그 등으로 확대되고, 인증대상도 사람에서 기기 등으로 확대된다.

아울러 u-IT 서비스가 활용되기 전에 개발단계에서부터 사전 보안성을 철저히 진단할 수 있는 체계 마련이 필요하다. 특히 전자정부와 같이 전 국민의 일상생활에 중요한 IT 서비스에 대해서는 시스템의 계획, 개발, 운영 등 전 단계에서 보안취약성을 점검할 수 있는 체계를 마련하여야 한다.



(그림 3) 융 · 복합서비스와 u-인증체계 구축

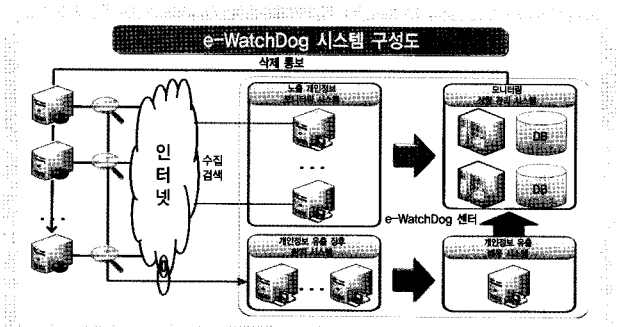
이처럼 신규 IT 서비스의 안전성과 신뢰성을 확보함으로써 IT 서비스의 보급과 활용도를 증가시키고, 다양한 기기가 연결되는 유비쿼터스 환경에서 이음새 없는 안전한 인증서비스 제공이 가능해질 것으로 전망된다.

다. 개인정보 침해 예방 및 대응체계 고도화

최근 옥션 해킹 등 개인정보의 유출로 인한 사회적, 경제적 피해가 증가하고 있다. 구글 검색 및 공공 · 민간 웹사이트에서 주민등록번호 등 개인정보의 노출이 지속적으로 발생하고 있으며, u-health 등 융합서비스가 활성화되는 시점에는 의료정보, 위치정보 등 다양한 개인정보의 유출로 인한 피해가 심각해 질 것으로 우려된다. 이에 따라 개인정보침해에 대한 예방 및 대응체계 고도화가 시급한 상황이다.

개인정보보호 체계를 강화하고, 이용자의 프라이버시를 보다 적극적으로 보호하기 위해서는 첫째, 개인정보 수집 및 관리체계를 정비하여 개인정보 수집 및 취급 행태 분석 등을 통한 개인정보 수집을 최소화할 수 있도록 강화하고, 인터넷상 주민번호 대체수단(민간 · 공공 i-PIN) 이용이 활성화될 수 있도록 지원을 강화하여야 한다. 둘째, 개인정보 유출 방지 대응체계를 강화하기 위해 인터넷상 개인정보 유 · 노출 탐지시스템(e-WatchDog)을 구축하고, 개인정보 관리 및 대응체계 점검을 위한 개인정보보호 인증제도 도입이 긴요하다. 셋째, 사업자의 책임성 강화 및 이용자 피해구제

환경을 정비하기 위해 개인정보보호 관련 기본법을 제정하고, 중요 개인정보 암호화 보관 의무화 등 개인정보보호를 위한 규정을 강화하여야 한다.



(그림 4) e-WatchDog 시스템 구성도

아울러 신규 IT 서비스 활용에 따른 이용자의 프라이버시 보호를 강화하기 위해, 개인정보를 수집 · 활용해야 하는 신규 IT 서비스에 대한 개인정보영향평가를 실시하고, 개인정보 수집 · 활용에 대한 구체적 기준 및 가이드라인을 개발하여 보급할 필요가 있다. 이러한 활동을 통해 개인정보 수집, 활용에 대한 이용자 자기정보 통제권을 강화하고, 개인정보 침해에 대한 사전예방 기능을 강화하여 사회적 손실을 최소화하며, 법제도 정비 및 피해구제 강화를 통해 사업자 책임이 강화되고 이용자 권리 구제도 향상될 것으로 기대된다.

라. 스팸 최소화를 통한 정보통신 이용환경 개선

이메일 및 휴대폰 스팸은 이용자들의 불편을 유발하고, 국가적으로도 막대한 피해를 끼치고 있다. 최근에는 부재중 전화 발신표시를 남김으로써 수신자의 호기심을 자극하는 '원링' 기법이나, 중국 등 해외에서 인터넷전화를 이용한 음성 스팸이 증가하고 있으며, 성인광고 및 대출광고, 대리운전 광고 등이 기승을 부리고 있다. 이에 따라 건전한 정보통신 이용환경을 조성하기 위해 스팸을 최소화하기 위한 대책이 중요하다.

스팸 발생을 최소화하기 위해서는 스팸 발생요인 억제를 통한 사전예방 체계 고도화가 중요하다. 통신사간 악성스패머 정보 공유를 통한 반복적인 서비스 재가입을 제한하고, 사업자 관리 · 감독 강화를 통해 스팸방지 자율규제 활성화를 유도하며, 스팸차단기술 보급 및 광고 발송단계 필터링을 강화하여야 한다. 또한 불법스팸에 대한 사후 대응조치의 실효성을 제고하여야 한다. 전화광고 사전수신동의(Opt-in) 예외 축소 및 스팸규제를 일원화하고, 불법스팸 광고주에 대한 형사 처벌을 강화하고, 아태지역 주요 국가 실시간 스팸정보 공유체계를 구축할 필요가 있다.

이러한 스팸 최소화 노력을 통해 악성 스팸행위가 감소됨으로써 정보통신을 이용하는 국민의 편의가 증진되고, 이메일 스팸 주요 발송국가라는 오명에서 탈피할 수 있을 것으로 기대된다.

3. 정보보호 기술, 제품, 산업간 선순환 촉진과 성장

기술이 경쟁력 있는 제품 개발을 촉진하고, 제품은 산업 활성화를 견인하는 선순환 구조를 마련하여 u-IT정보보호 기술 개발, 국제 표준화, 고등급 평가 수행 등 국내 제품 · 서비스의 글로벌 경쟁력을 확보함으로써 지속적인 산업성장에 기여하는 체계를 정립해야 한다.

가. 지식정보보안산업의 글로벌화를 위한 성장기반 조성

국민의 공익성과 타산업으로의 파급효과가 막대한 지식정보보안산업을 체계적으로 육성하여 보안주권을 확보하고 시장을 선점하기 위해서는 정부의 다각적인 정책적 지원이 중요하다. 구체적으로 지식정보보안 R&D 및 표준화 역량 강화, 전문인력 양성 등을 통해 국제적 수준의 정보보호제품을 개발하고, 보안산업 스타기업을 육성할 필요가 있으며, 이를 뒷받침하기 위한 법제도적 장치 마련이 요구된다.

아울러 지식정보보안제품 시험환경 구축, 성능 · 품질 인증서비스를 지원하는 한국정보보호진흥원의 산업지원센터 기능을 확대하여 바이오인식 제품 외에 웹방화벽, IPS 등 네트워크 · 시스템 제품군 시험인증 서비스 등을 제공할 필요가 있다. 또한 지식정보보안산업 시장 활성화를 위해 정보보안 제품 도입, 컨설팅서비스 지원 등 국가 차원에서의 시범사업을 적극적으로 추진하고, 해외진출, R&D공동 개발 등 국가기업 간 의견교환 및 지원 창구 등 산업지원 컨트롤타워 역할을 강화하여야 한다.

이러한 활동들을 통해 지식정보보안 제품의 안전신뢰성을 확보하고 국제 경쟁력을 개선하여 2010년 5조원 규모로 국내 지식정보보안시장이 활성화되고, 국내제품의 국외수출도 크게 증가할 수 있을 것으로 기대된다.

나. 안전한 u-IT 서비스를 위한 핵심 보안기술 개발

신규 융합 서비스의 역기능을 사전에 방지하기 위해 VoIP, IPTV 등 u-IT 신규 서비스에서 사용자의 프라이버시 보호 및 장애방지 기술을 개발하여 적용하고, 융합 서비스에 적합한 능동형 탐지 · 대응 기술을 조기에 확보하여야 한다.

또한 융합 서비스에 적용할 수 있는 개인정보 자기통제권이 강화된 차세대 전자ID 시스템을 개발하고, SSL 등 인터넷 보안통신에서 국내 암호기술 이용을 확대할 필요가 있다. 아울러 국제적인 기술선도를 위해 바이오인식, 모바일 보안 등 국제적으로 IT 경쟁력이 높은 분야를 선정하여 국가 주도로 기술 및 제품 개발을 개발하고, 임베디드 제어 보안기술, IT-공간 융합형 통합보안 등 신기술을 조기에 확보하는 것이 중요하다. 이와 같이 안전한 u-IT 서비스에 적합한 핵심 보안기술을 개발 및 확보함으로써 VoIP, RFID/USN 등 신규 융합 서비스의 경쟁력을 강화하고 이용이 활성화될 것으로 기대된다.

다. 안전한 정보시스템 이용기반 조성

유비쿼터스 환경에서는 이동기기, 스마트카드, 정보가전 등 다양한 디바이스의 활용이 증가하고, 이러한 디바이스가 컴퓨팅 및 네트워킹 기능을 보유하게 된다. 이에 따라 정보시스템의 안전한 이용을 이용해서 디바이스의 보안성 평가 기술을 확보하는 것이 중요하다. 이를 위해 EAL5등급이상 고등급 평가방법론 및 평가기술을 확보하고, 고등급 평가가 요구되는 IC칩 등 디바이스 평가기술을 확보하며, 디바이스 평가를 위한 시험환경을 구축하는 것이 요구된다.

아울러 해외 선진 평가 기관과 국내 유사 시험 기관과의 유기적 협력을 통해 기술력을 제고하고, 독자적 IC칩 평가 능력을 확보함으로써 아시아 최고의 고등급 평가기술을 보유할 수 있을 것으로 전망되며, 정보보호제품의 국제경쟁력 제고에도 큰 도움이 될 것으로 기대된다.

IV. 결 론

다가오는 지식정보사회는 인간의 편리함과 안락함을 향상시키지만, 고도화된 IT 활용이 오히려 프라이버시 침해, 정보오염 등 역기능을 심화시키고, 인간의 자유와 표현을 억제할 수 있는 가능성도 배제할 수 없다. 따라서 향후 지식정보사회에서 밝은 미래를 맞이하기 위해서는 사전에 다양한 역기능을 예측하여 미연에 방지하기 위한 다각적인 노력을 전개하여야 한다. 다양한 미래 IT 위협에 대비하기 위해서는 다양한 정보 주체의 참여와 협력기반으로 중장기적 정보보호 정책 및 전략을 설정하고, 구체적인 실행방안을 마련하여 적극적으로 추진하여야 한다.

아울러 방통융합 등 IT 환경이 지속적으로 변화하고 신종 사이버위협이 출현이 증가함에 따라 중장기 정보보호 정책 및 전략 추진의 효과성을 주기적으로 분석하여 지속적으로 개선할 필요가 있다. 이를 위해 정보보호 정책의 효과성을 분석하고, 합리적인 정책 의사결정을 지원할 수 있는 계량화된 정책성과 평가모델의 개발 및 활용이 요구된다.

이러한 정보보호 노력을 통해 우리나라는 2012년에 국가정보보호지수를 80점까지 향상시키고, 전자거래의 신뢰성을 표시하는 보안서버 지표 순위를 전 세계 5위 이내로 높이고, 정보보호기술수준도 선진국 대비 95% 수준까지 제고할 수 있을 것으로 예측된다. 아울러 개인정보 노출도 최소화되어 IT서비스 활용 증대에 따른 국민의 프라이버시 침해 우려도 대폭 해소될 것으로 기대한다. 2012년, 한국은 세계적인 정보보호 선도국가로 도약하여 국제사회에서 가장 앞서 고도의 정보신뢰사회를 구현할 수 있을 것으로 기대된다.

약 력

황 중 연

1972년 마산고등학교 졸업
1977년 영남대학교 법학과 졸업
1992년 영국시티대학
1996년 미국 콜로라도대학
1997년 ~ 1998년 정보통신정책실 기술심의관
1998년 ~ 1998년 정보통신부 공보관
1998년 ~ 1999년 정보통신부 국제협력관
1999년 ~ 2000년 정보통신부 우정국장
2000년 ~ 2001년 정보통신부 전파방송관리국장
2001년 ~ 2005년 부산, 서울체신청장
2005년 ~ 2007년 정보통신부 우정사업본부장
2007년 ~ 현재 한국정보보호진흥원장
행정고시 20회
1986년 근정포장
2000년 홍조근정훈장