유비쿼터스 환경변화에 따른 정보보호의 주요 현황과 대응전략

황중연
한국정보보호진흥원

요 약

국가사회기반구조의 중추신경계 역할을 수행하는 정보통신 인프라를 기반으로 개인의 사이버생활 일상화, 디지털경제로의 전환, 전자정부 구축이 가속화되고 있다. 또한 네트워크 통합과 정보통신 서비스의 융합 등을 통한 제2의 디지털 혁명으로 유비쿼터스 사회가 도래하고 있다.

그러나 이와 더불어 정보보호 환경은 개별 시스템, 네트워크 보호에서 서비스와 이용자 보호로 그 중심이 급격히 옮겨져 그 범위가 크게 확대되고 있으며, 웜 · 바이러스와 해킹 기능의 결합으로 복합화(Blended), 악성화된 사이버공격이 증가하고 있다.

또한 그 전파경로가 이메일은 물론 PC의 공유폴더, P2P, 웹 등으로 확대됨으로써 피해범위는 유선단말에서 무선단말과 방송단말 등으로 확장되고 있다.

이처럼 시간과 장소에 상관없이 지식정보를 자유롭게 이용함으로써 편리하고 쾌적한 정보이용 환경을 누리게 하는 유비쿼터스 사회는, 그러나 동시에 예측 불가능한 위험이 곳곳에 산재한 '고도화된 정보위험사회'로의 진입을 의미한다. 이에 따라 새로운 위협이 상존하는 유비쿼터스 환경하에서 안심하고 신뢰할 수 있는 새로운 정보보호 정책방향의 설정과 대응전략이 필요함은 주지의 사실이라고 할 수 있다.

이에 본고에서는 유비쿼터스 사회에서 나타나는 새로운 도전과 신규위협에 대해 살펴보고, 정보보호 3대 핵심 추진방향을 비롯한 향후 대응전략과 이를 통한 안전한 미래 사회의 청사진을 제시하도록 한다.

I. 서 론

국가사회기반구조의 중추신경계 역할을 수행하는 정보통신 인프라를 기반으로 개인의 사이버생활 일상화, 디지털경제로의 전환, 전자정부 구축이 가속화되고 있다. 또한 네트워크 통합과 정보통신 서비스의 융합 등을 통한 제2의 디지털 혁명으로 유비쿼터스 사회가 도래하고 있다. 그러나 이와 더불어 사이버공격 범위가 확대되고 공격형태가 다양화되면서 첨단 인프라에 대한 위협이 확산되고 있다. 사이버공격으로 인한 개별망의 피해가 유 · 무선 통합망으로 확산되고 나아가 방송망과 센서네트워크, 댁내 망까지 확산될 공산이 매우 커지고 있다. 또한 지난 10년간 정보보호 환경은 개별 시스템, 네트워크 보호에서 서비스와 이용자 보호로 그 중심이 급격히 옮겨져 그 범위가 크게 확대되고 있다. 웜 · 바이러스와 해킹 기능의 결합으로 복합화(Blended), 악성화된 사이버공격이 증가하고, 아울러 그 전파경로가 이메일은 물론 PC의 공유폴더, P2P, 웹 등으로 확대됨으로써 피해범위는 유선단말에서 무선단말과 방송단말 등으로 확장되고, 이에 따른 사이버 역기능 또한 급격히 증가하고 있다. 더불어 비윤리적 · 반사회적 · 정보침해 내용의 콘텐츠들이 개방된 네트워크를 통해 급속히 전파되면서 사이버공간의 심각한 사회 · 문화적 부작용을 야기하고 있다.

최근 분석에 따르면, 인터넷 침해사고로 인한 경제적 손실은 연간 약 4,500억 원에 이르는 것으로 나타난 바 있다. 아울러 웹2.0, UCC 등 쌍방향 웹서비스 확대로 개인정보의 유출이 심각한 사회문제로 대두되고 있다. 이처럼 인터넷침해

와 무차별적으로 살포되는 악성스팸, 개인정보침해 등 사회 경제적 손실을 야기하는 사이버 역기능과 위협이 점차 지능화되고 고속화되고 있다.

이처럼 시간과 장소에 상관없이 지식정보를 자유롭게 이용함으로써 편리하고 쾌적한 정보이용 환경을 누리게 하는 유비쿼터스 사회는, 그러나 동시에 예측 불가능한 위험이 곳곳에 산재한 '고도화된 정보위험사회'로의 진입을 의미한다. 즉, 고도화되고 복잡해진 정보기술이 사회시스템의 핵심 기반으로 자리 잡게 되고 디지털 컨버전스가 확대되면서 특정 기술의 약한 고리에서 발생한 위험이 도미노 현상을 일으켜 전 사회의 위기로 몰아 갈 수 있는 잠재적 가능성이 상존하고 있다.

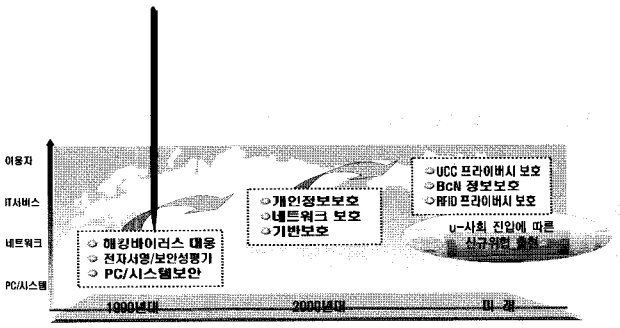
이에 따라 새로운 위협이 상존하는 유비쿼터스 환경 하에서 안심하고 신뢰할 수 있는 새로운 정보보호 정책방향의 설정과 대응전략이 필요함은 주지의 사실이라고 할 수 있다. 이에 본고에서는 유비쿼터스 사회에서 부상하는 새로운 도전에 대해 살펴보고, 향후 정보보호 대응전략과 이를 통한 안전한 미래 사회의 청사진을 제시하도록 한다.

II. 정보보호 환경 변화

1. 유비쿼터스 사회의 새로운 도전

가. 시스템, 네트워크 보호에서 서비스와 이용자 보호로 확대

기존의 정보보호는 시스템과 네트워크 보안을 중심으로 하는 사업자 일방형이었으나, 점차 일반 이용자의 정보 단말과 서비스 중심의 정보보호로 변화하고 있다. 또한 기존 유선망 중심의 인터넷 기반의 정보보호에서 컨버전스 네트워크상의 정보보호로 변화가 이루어지고 있다. 이에 따라 속도와 서비스의 품질(QoS, Quality of Service)이 중요시 되었던 광대역 망에서 이제는 이음새 없고 이동성과 보안, 그리고 프라이버시가 강조되는 유비쿼터스 네트워크로 진화되고 있다.



(그림 1) 정보보호의 범위 확장

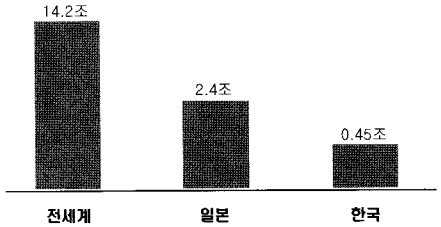
나. 웹2.0, UCC[1], RFID[2] 등 유비쿼터스 IT 환경에서의 신규위협 출현

웹2.0과 UCC, RFID 등은 현재 널리 이용되고 IT 패러다임으로 자리잡아가고 있지만, 이미 웹2.0을 통한 저작권 침해와 프라이버시 침해와 같은 다양한 역기능이 발생하고 있으며 보안 전문가들이 해당 기술들의 취약점에 대해 경고하는 등 예측 불가능한 새로운 정보 위험 요소로 자리 잡고 있다. 또한 블로그와 소셜 네트워크 등에서 발생하는 개인정보 침해와 Ajax[3], RSS[4] 같은 신기술의 다양한 취약점을 이용한 악성코드 유포 등의 문제가 대두되고 있다.

2. 사회 · 경제적 손실의 심화

가. 웜 · 바이러스 등 인터넷 침해사고로 인한 경제적 손실 심화

인터넷 침해사고로 인한 국내 기업의 2005년 연간 누적 피해액은 약 4,500억 원인 것으로 조사되었으며, 2003년 발생한 1.25 인터넷 침해사고의 경우 단일 사고로만 약 1,700억 원의 손실이 발생한 것으로 나타났다.



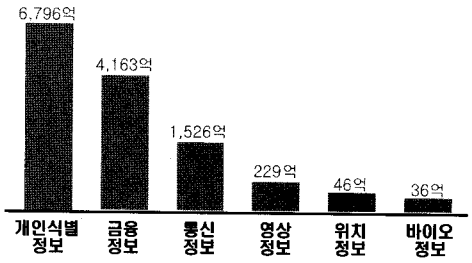
(그림 2) 인터넷 침해사고로 인한 경제적 손실규모

01_ User Created Contents
02_ 소형 반도체 칩을 이용해 사물의 정보와 주변 환경정보를 전송?처리하는 비접촉식 인식시스템
03_ 대화식 웹 애플리케이션의 제작을 위해 사용되는 개발기법
04_ 뉴스나 블로그 사이트에서 주로 사용하는 콘텐츠 표현 방식

우리나라의 GDP 대비 인터넷 침해사고 피해액 비율은 전 세계 평균의 1.8배로 매우 높으며, 일본보다는 약간 높은(1.1배) 수준으로 향후에는 그 규모가 더욱 확대될 것으로 우려된다.

나. 새로운 기술의 등장에 따른 프라이버시 침해 우려 등 개인정보보호의 중요성 증대

개인정보 유출 피해 회피를 위한 연간 지불의사 금액은 개인 47,000원, 국가 전체 1조 3천억 원에 이른다. 향후 유비쿼터스 사회가 본격적으로 대두되면서, UCC와 SNS[5] 등을 통한 개인정보 유출과 침해가 심각해 질 것으로 우려되고 있다.

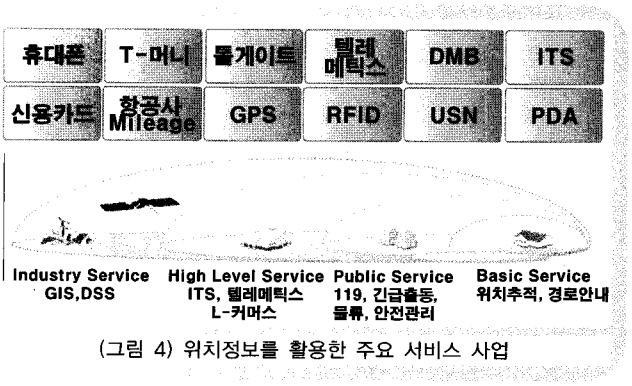


(그림 3) 개인정보의 자산 가치

3. 신규 IT 서비스에 대한 보호대책 마련 필요

민감한 개인정보를 활용한 신규 IT 서비스로 역기능 발생 가능성이 증대되고 있다. 이로 인한 국민적 우려 및 피해방지를 위한 대책이 요구된다. 특히 위치정보서비스(LBS)는 개인의 주요 활동반경이나 이동방향, 취미, 관심사까지도 예측할 수 있는 단서를 제공한다. 위치정보서비스는 개인 활동정보가 중앙 DB에서 집중관리 됨에 따라 이에 대한 제도적 관리가 필요하다.

한편 바이오 정보는 신체로부터 획득한 유일한 식별자로서 망막, 홍채, 음성, 손등 정맥, 유전자, 족문 등의 바이오정보 축적을 통해 실시간 추적과 감시가 가능하다. 더욱이 최근 세계적으로 전자여권, 전자주민증 등에서 신원확인시스템으로 도입되는 사례가 증가하고 있어 이에 대한 국가차원의 체계적이고 투명한 관리체계 마련이 필요하다.



(그림 4) 위치정보를 활용한 주요 서비스 사업

III. 정보보호 3대 핵심 추진방향

1. 안전한 u-사회 청사진 설계 및 환경조성

가. 유비쿼터스 사회의 위협 예측 및 정보보호 정책개발

안전한 유비쿼터스 사회 구현을 위해서는 우선 체계적인 대응책을 마련하고, 이에 대한 전략적 추진방향 설정이 필요하다. 이를 위해 정치, 경제, 사회, 문화 등 다양한 분야에서 나타날 것으로 예측되는 미래위협을 도출하고, 산·학·연·관 협업 체계 구축을 통해 유비쿼터스 사회 정보보호의 큰 흐름들에 대한 선행연구가 필요하다. 더불어 웹2.0과 융·복합시대에 적합한 정보보호의 새로운 패러다임을 정립하고 개별 이용자의 인식제고와 정보보호 서비스의 원활한 이용을 위한 다양한 정책적 대안들이 마련되어야 한다.

아울러 민간분야 뿐만 아니라 공공분야 정보보호 체계 강화를 위해 긴밀한 협조체계를 구축하고, 세계 수준의 연구기관과의 글로벌 협력 네트워크 구축을 통해 스팸과 인터넷 침해사고와 같이 국경 없이 넘나드는 사이버 위협에 적극 대처할 필요가 있다.

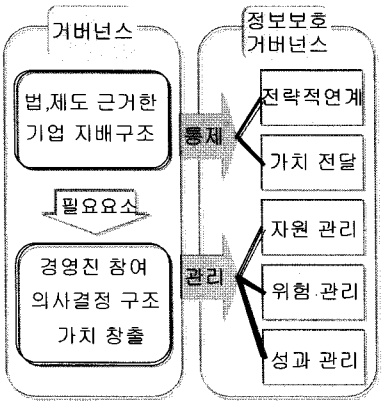
나. 기업 유형별 정보보호 거버넌스[6] 체계 정착

사회 전반의 전방위적 정보보호 강화를 위해서는 민간부

05_ Social Networking Service 또는 Social Networking Sites로 사회적 친목도모를 위한 인터넷 웹 서비스
06_ 기업의 전략과 목표에 부합되도록 정보보호와 관련된 IT자원 및 프로세스를 통제, 관리하는 체계

문에서의 자발적인 정보보호 활동이 반드시 선결되어야 하며, 이를 위해서는 정보보호가 기업 경영활동의 핵심과정으로 포함되고 최고경영층의 적극적인 참여와 지원을 유도할 수 있는 정부의 정책 개발이 요구된다고 할 수 있다. 이에 따라 기업의 정보보호 거버넌스 도입을 촉진하기 위해 정보보호 거버넌스 프레임워크를 개발하고, 투자 대비 효과성을 검증할 수 있는 측정 척도 개발 및 적용, 그리고 의료, 교육 등 분야별 특성을 고려한 위협 프로파일 개발 등을 추진할 필요가 있다.

아울러 웹 서비스 기업의 정보보호 거버넌스 도입 촉진을 위해 취약성이 많은 웹을 대량 취급하는 웹서비스 업체가 상시적으로 취약점을 점검할 수 있도록 정보보호 관리체계 수립과 인증 취득을 위한 제반 활동을 지원하는 것이 중요하다. 이를 통해 기업의 정보보호 실효성을 제고하고 사회 전반의 정보보호의 수준을 보다 강화할 수 있을 것으로 기대된다.



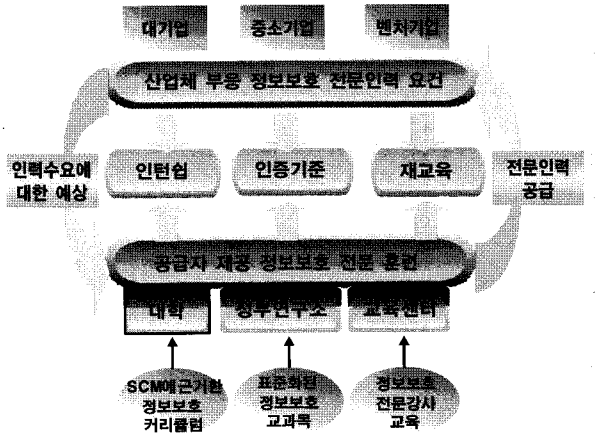
(그림 5) 정보보호 거버넌스 구성

다. 미래 유망 IT 분야의 정보보호 핵심인재 양성

새로운 IT 서비스의 개발과 이용이 증가함에 따라 정보보호 취약점 노출방지기술 개발과 정책마련을 위한 정보보호 인력의 원활한 공급체계를 마련하는 것이 중요하다. 이를 위해서는 1차적으로 현재 나타나고 있는 인력수급의 불균형 현상을 해소하고 향후 산업체 수요에 적합한 핵심 정보보호 인력 양성체계 프로세스를 갖추는 것이 필요하다.

구체적으로 수요 맞춤형 정보보호 핵심인력 양성체계(SCM) 구축을 통해 인력수급 조사 · 전망 체계개발과 더불어 정보보호 인력통계에 대한 DB를 구축하여 운영하고, 산업체와 대학의 인력을 대상으로 수요 · 공급 정보를 공유할 수 있도록 조정하는 것이 중요하다.

또한 정보보호 인력양성을 위한 교육지원센터 구축과 이를 통해 기존 IT 인력, 정보보호 취약계층, 초 · 중 · 고 교사, 정보보호 관련 동아리 등에 대한 특성화된 교육서비스를 제공하고, 교육기관과 해당 과정에 대한 평가인증 지원, 정보보호 자격제도 운영, 인력양성 정책개발 등을 통합하여 수행할 수 있는 지원체계를 마련하는 것이 필요하다.



(그림 6) 정보보호 핵심인력 양성체계 구축을 위한 구조

이를 통해 산업체가 직접적으로 필요로 하는 기술과 직무능력을 갖춘 인재를 적시에 공급할 수 있는 기반을 마련하고, 국가경쟁력의 원천인 핵심인력을 확보함은 물론 일반인에 대한 정보보호 리터러시(Literacy)를 함양할 수 있는 계기가 될 것으로 기대된다.

2. 사이버위협 예방 및 대응체계의 입체적 조화

가. 광대역 융합 네트워크(BcN)의 종합해킹대응시스템 구축

인터넷 침해사고로 인한 경제적 피해를 대폭 감소시키기 위해 네트워크 침해사고에 대비한 종합해킹대응체계를 구축하는 것이 필요하다. 구체적으로 먼저 네트워크 분야에서는 악성봇, 악성트래픽 모니터링 등 네트워크 위협 대응체계를 강화하고, 서비스 · 응용분야에서는 웹 어플리케이션

공격, 피싱 탐지 시스템을 구축하는 것이 필요하다. 아울러 사고 원인의 상관관계 분석을 통해 침해사고 추적과 원인제거를 위한 전방위적 체계를 구축하는 것이 중요하다.

또한 국내 ISP 사업자의 국내 연동망과 분산서비스거부(DDoS) 공격에 대비한 DDoS 클리어링 시스템 구축 및 상호 연동을 통해 복수 ISP 연동구간에서 DDoS 대응체계를 구축하고 3세대(3G) 휴대폰, 센서네트워크의 인터넷 연동에 따른 위협 분석과 대응체계 강화를 통해 무선 환경에서의 침해사고 대응체계를 구축하는 것이 필요하다.

이러한 활동을 통해 악성봇 감염률을 10% 이하로 감소시킬 수 있으며, 악성코드 은닉 재발률을 20% 이하로 개선할 수 있을 것으로 기대된다. 아울러 협박성 DDoS 방어능력 및 대응체계 확보를 통해 국내 인터넷 서비스 기관을 보호할 수 있는 기반을 마련할 수 있을 것으로 예측된다.

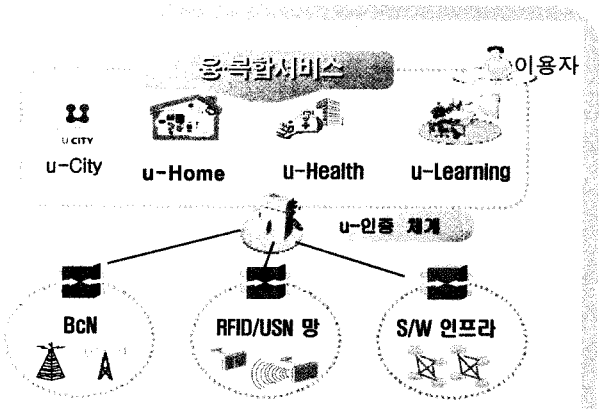
나. 융 · 복합 서비스의 안전 · 신뢰성 강화

현재 우리나라의 공인인증서비스 이용자 수는 1,600만 명에 이르러 온라인상의 안전한 거래를 위한 기반은 어느 나라보다 잘 마련되어 있다고 할 수 있다. 그러나 새로운 융 · 복합 서비스가 출현하고, 이에 대한 안전과 신뢰성의 문제가 지속적으로 제기됨에 따라 공인인증서 이용자수를 2010년에 전체 인터넷 이용자의 60%에 이르는 2,000만 명까지 확대할 필요가 있다.

아울러 최근 떠오르고 있는 u-City에 대한 u-IT 서비스 정보보호 진단 및 제도화 추진, u-IT 인프라라고 할 수 있는 BcN, RFID, USN 등에 대한 보호대책 개발과 점검을 추진하고 주요 웹, 공개 및 임베디드 소프트웨어 등의 취약점 분석, 온라인 소프트웨어(SaaS)의 무결성을 보장하는 기술개발과 적용노력이 필요하다. 또한 u-IT 서비스의 기반 소프트웨어 보안성을 강화하기 위해 정보공유 및 검증, 패치경보체계 구축과 운영 등이 필요하다.

그리고 인증수단을 현재의 PKI기반에서 바이오정보, 전자태그 등으로 확장하고, 인증대상을 사람에서 기기와 사물까지로 확대함으로써 신뢰 이용환경 제공을 위한 u-인증체계가 마련될 수 있을 것으로 기대된다.

이처럼 소프트웨어의 안전성과 신뢰도 제고를 통해 그 활용이 더욱 촉진되고, 사람은 물론 다양한 기기가 연결되는 유비쿼터스 환경에서 이음새 없는 안전한 인증서비스 제공이 가능해질 것으로 전망된다.



(그림 7) 융 · 복합서비스와 u-인증체계 구축

다. 이용자 프라이버시 보호체계 고도화

개인정보 노출을 대폭 감소시키고 이용자 프라이버시를 보다 적극적으로 보호하기 위해서는 첫째, 이용자의 편의성을 높인 민원처리 서비스 품질 향상과, 개인정보 침해에 대한 법 집행력을 강화하는 것이 중요하다. 둘째는 이용자 자기정보 통제기술 개발로서, 개인정보취급방침을 손쉽게 확인할 수 있는 에이전트 소프트웨어의 보급, 개인위치정보 수집시간 제한 등 이용자 자신이 자신의 프라이버시 보호 정도를 자율적으로 설정할 수 있는 소프트웨어의 개발, 그리고 개인정보 노출 실시간 모니터링 및 삭제요청 자동화 시스템 구축 등이 긴요하다. 한편 사업자의 자율적인 프라이버시 보호활동을 지원하기 위해 IPTV, UCC 등 개인영상정보 보호 가이드 제정과 보급, RFID, 바이오인식 시스템 도입기관의 개인정보 영향평가 등을 확대하는 것이 바람직하다.

이러한 계획을 통해 개인정보 수집, 활용에 대한 이용자 자기정보 통제권을 강화하고 개인정보 침해에 대한 사전예방 기능 강화를 통해 사회적 손실을 최소화할 수 있을 것으로 기대된다.

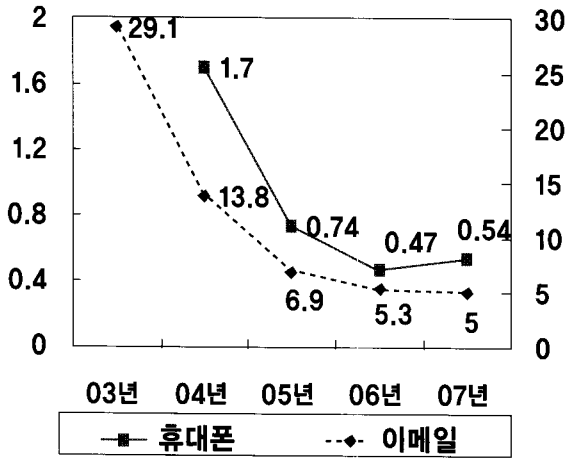
라. 스팸 최소화를 통한 정보통신 이용환경 개선

현재 5통인 이메일스팸 수신량과 0.54통인 휴대전화 스팸 수신량을 향후 대폭 감소시키기 위해 온라인 스팸규제 관련 법 개정을 통한 규제 단일화를 추진하고, 불법스팸으로 인해 발생할 수 있는 정상적인 광고의 피해방지를 위해 화이

트리스트(White-list)를 보급함으로써 불법스팸에 대한 적발을 강화할 필요가 있다.

아울러 정보통신 컨버전스에 따른 신종스팸 대응기술을 확보하기 위해 능동형 학습기능을 이용한 이미지스팸 자동탐지 · 차단기술 개발하고, 휴대전화 URL-SMS스팸 등에 대한 자동분석 · 정보추출 기술을 확보하는 것이 중요하다.

한편 악성 스패머 조회시스템 개발을 통한 사업자간 정보공유 체계 구축, 해외 경유 스팸정보에 대한 국가간 정보공유 시스템 구축 등을 통해 사업자들이 자율적으로 스패머의 정보통신서비스 이용을 제한하도록 유도하는 것이 바람직하다.



(그림 8) 휴대폰, 이메일 스팸 수신량 추이

아울러 현재 공정거래위원회와 정보통신부 등으로 2원화되어있는 스팸 고충처리 창구를 정보통신부로 일원화함으로써 국민 편의를 증진시키고, 악성스패머의 유사 서비스 재가입을 이용한 스팸발송을 40% 정도 감소시킴으로써 이메일스팸 발송 3위 국가라는 오명을 탈피할 수 있을 것으로 기대된다.

3. 정보보호 기술, 제품, 산업간 선순환 촉진

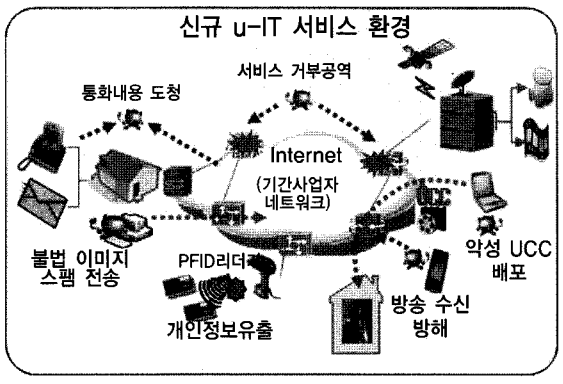
가. 정보보호 산업육성 및 글로벌 경쟁력 강화

국내 정보보호산업 육성을 위해서는 정보보호촉진관련 법 · 제도 정비, 인수합병(M&A) 등 산업경쟁력 지원정책을 도출하고, 정보보호 수요확대를 위한 우선구매제도 도입과 세제지원을 확대하는 것이 필요하다. 아울러 한국정보보호진흥원내에 설치되어 있는 정보보호산업지원센터의 기능을 현재 시험환경 단순 제공기능에서 성능품질 인증 시험서비스를 제공하는 종합지원센터로 확대하는 것이 필요하다.

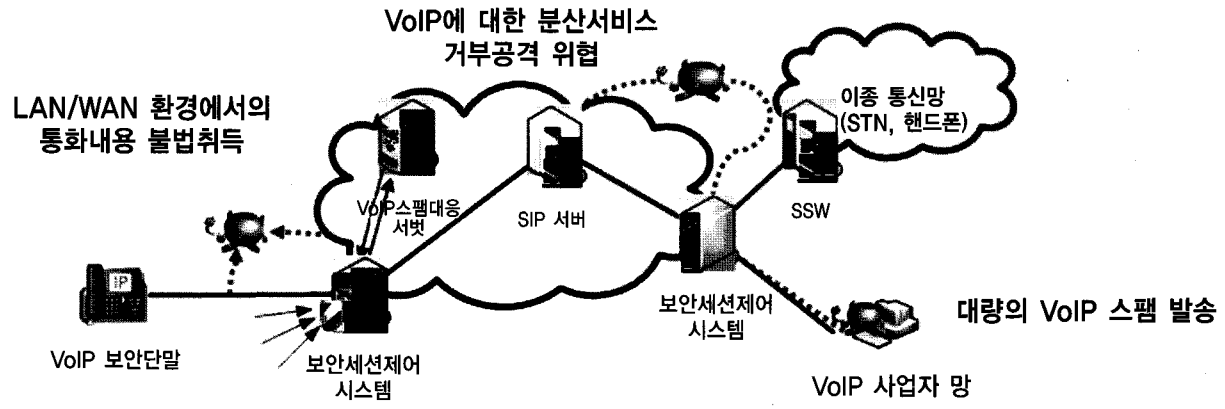
한편 한국정보보호진흥원의 바이오인식정보시험센터(K-NBTC) 국가공인과 국제공인을 획득하고 시험기술의 국제공동연구를 통해 관련 기술의 선진화를 도모하고, 국제표준을 선점함으로써 아시아 허브로 도약할 계기를 마련할 수 있을 것으로 기대된다. 이러한 활동들을 통해 국내 정보보호 시장 규모는 2010년까지 연평균 10% 성장률을 기록하여 1조원 규모에 이를 것으로 전망되며, 2012년에 이르면 세계 바이오인식 3대 기술강국 진입과 1,500억 원 규모의 시장을 조성할 수 있을 것으로 예측된다.

나. u-IT 서비스의 안전한 이용을 위한 보안기술 개발

VoIP, IPTV와 같은 u-IT 신규 서비스에서 사용자의 프라이버시를 보호하고, 서비스 장애 방지 및 지식정보의 안전한 유통을 위한 기술 개발 등을 통해 신규 융 · 복합 서비스의 역기능을 방지할 수 있을 것으로 기대된다. 아울러 개인정보의 자기통제권이 강화된 차세대 전자ID 시스템 구축을 추진하고 향후 경제적 파급효과가 클 것으로 예측되는 IP-USN과 같은 신규 보안기술의 국내외 표준화를 추진하는 것이 중요하다. 이러한 제반 활동을 통해 신규 융 · 복합 서비스 이용 확산과 시장 활성화는 물론, 국내 우수 정보보호기술의 경쟁력 강화, 국제적 인지도 제고와 함께 다수의 국제표준화, 기술이전, 특허 등의 성과를 달성할 수 있을 것으로 기



(그림 9) 신규 u-IT 서비스 환경의 정보보호 위협



(그림 10) VoIP 보안위협

대된다.

한편 최근 크게 조명 받고 있는 IP기반 VoIP 서비스는 인터넷 망에서의 보안위협에 그대로 노출될 수 있어 불법도청, 스팸, 장애를 사전에 예방하기 위한 정책지원 및 기술대책이 필요하다. 이를 위해 관련 서비스 제공업자를 주요정보통신기반시설로 지정하고, 사업자 대상 보안교육 등을 추진하는 것이 바람직하다.

아울러 VoIP 스팸탐지 기술, 암호 및 키관리 기술 등 기술적 노력과 함께 VoIP 스팸대응기술을 ITU-T 신규표준으로 제안하는 등 국내외 표준화를 통해 기술과 산업의 경쟁력 강화를 유도할 필요가 있다.

다. 안전한 u-디바이스 제품 이용기반 조성

다양한 단말기의 안전성을 확보하기 위해서는 디바이스 보안성 평가기술의 확보가 무엇보다 중요하다. 이를 위해 EAL5등급이상 고등급 세부 평가방법론과 취약성 평가 방법론을 개발하고 이에 맞는 평가환경을 구축하는 것이 필요하다. 아울러 해외 선진 평가 기관과 국내 유사 시험 기관과의 유기적 협력을 통해 기술력을 제고하고, 가까운 미래에 독자적 IC칩 평가 능력을 보유함으로써 세계 5위권 정도의 정보보호시스템 평가국으로 성장함으로써 아시아 최초의 고등급 평가기술을 보유할 수 있을 것으로 전망된다.

이러한 활동을 통해 유비쿼터스 환경에서 개인정보 유출 등 침해 사고 예방은 물론 첨단기술 유출방지 및 국내 제품 수출 경쟁력 강화를 통해 국가 경쟁력 제고에도 큰 도움이 될 것으로 기대된다.

IV. 2008년도 주요 사업 추진방향

2008년도 한국정보보호진흥원의 주요 사업은 크게 정보보호 인프라 강화, 해킹 · 바이러스 대응체계 고도화, 개인정보보호 강화, 전자서명관리, 기업 정보보호 대응능력 강화, 정보보호 산업경쟁력 강화 등으로 나누어 볼 수 있다.

먼저 정보보호 인프라 강화를 위해서 진흥원은 산학연관의 다양한 전문가로 구성된 정보보호 전략포럼을 통해 u-지식정보 사회 도래에 따른 새로운 정보보호 이슈를 발굴하고, 이에 대한 대응방안을 마련할 계획이다. 아울러 u-지식정보 사회의 다양한 변화상을 분석하고, 정보보호 취약계층의 인식 확산과 일반 네티즌의 정보 접근성 확대를 위한 정보보호 문화운동 전개할 예정이다.

또한 u-IT 시범 서비스에 대한 정보보호 사전진단, 서비스별 정보보호 참조모델 수립, 암호기술 이용 촉진을 위한 기술적 · 제도적 방안 마련 등을 통해 정부의 정보보호 정책마련과 민간의 사업계획 수립 시 참고할 수 있는 유용한 정보를 제공하고 정보보호의 중요성에 대한 사회의 인식을 크게 높일 수 있을 것으로 기대된다.

해킹 · 바이러스 대응체계 고도화를 위해 진흥원은 인터넷 침해사고 예방 · 분석 및 대응기술을 강화하고, 국내 · 외 침해사고 협력체계 및 공동 대응활동을 확대함으로써 안전한 인터넷 이용환경의 기반을 조성하는데 만전을 기할 예정이다.

온라인 개인정보보호 강화를 위해서는 RFID, CCTV 등 새로운 정보기술 취급사업자의 프라이버시 보호 가이드라인 준수율을 지속적으로 점검하고, 개인정보 취급관행 개선 여부를 위한 계도조치를 강화할 방침이다. 아울러 신규 위치기반서비스 및 시범사업의 위험 분석을 통해 프라이버시 침해 위협을 최소화하여 이용자 자신의 자기정보 통제권을 강화할 계획이다. 또한 인터넷 상에 노출된 주민번호 등 개인정보의 지속적인 삭제조치를 통하여 명의도용 등 개인정보의 추가적인 오 · 남용을 방지하고, 인터넷상의 개인식별보급번호(아이핀, *i*-Pin)와 보안서버의 이용확산을 통해 온라인상의 개인정보보호를 위해 만전을 기할 계획이다.

기업 정보보호 대응능력 강화를 위해 진흥원은 신규 IT 서비스 등 분야별 특성화된 정보보호관리체계 수립기반 환경을 조성하고, 기업의 정보보호관리 수준 제고 및 잠재적 고객 확보, 온라인 정보보호 강의 프로그램 보급 확대, 고객 중심의 인증 서비스 개선을 통해 고객 편리성과 만족도를 제고할 방침이다.

한편 정보보호 산업경쟁력 강화를 위해 진흥원은 현재 운영 중인 정보보호산업지원센터의 이용률을 개선하고, 바이오인식시스템 시험 및 인증서비스 제공, 정부(공공)기관의 바이오인식 시범사업 기술자문 서비스를 제공할 예정이다. 이와 함께 공정하고 객관적인 정보보호 제품에 대한 시험환경을 제공함으로써, 국내 정보보호 산업의 활성화와 더불어 국제경쟁력을 강화시킬 수 있을 것으로 기대된다.

V. 결 론

유비쿼터스 컴퓨팅 기술을 통해 만들어가는 정보환경은 인간의 편의를 위해 인위적으로 만들어낸 환경이지만, 이러한 기술적 진보는 오히려 인류의 자유와 표현을 크게 속박할 수 있는 가능성도 적지 않다. 따라서 향후 다가올 유비쿼터스 사회가 단지 유토피아적 미래상만을 우리에게 제시하는 것은 아니며, 발생할 수 있는 다양한 역기능을 미연에 방지하고 그 부정적 영향들을 최소화하기 위한 전방위적 노력이 경주되어야 한다. 아울러 정보보호가 다양하고 새로운 IT 서비스에 대한 불안을 해소하여 새로운 IT 시장 창출과 진흥에 기여하는 역할로 변모할 수 있을 것으로 전망된다.

이러한 노력을 통해 우리나라는 2010년에 현재 49위인 WEF 보안서버 지표를 5위까지 끌어올리고, 22위인 IMD 사이버보안 지표를 10위로 끌어올릴 수 있을 것으로 예측된다. 아울러 개인정보 노출을 현재의 1/10 이하로 감축하고, 바이오인식정보의 보호체계를 통한 유출 방지 등 주요 목표 달성을 통해 우리나라가 가지고 있는 IT강국 이미지에 걸 맞는 세계 최고의 정보보호 수준을 달성할 수 있을 것으로 기대된다.

약 력

황 중 연

1977년 영남대학교 법학과 졸업
1992년 영국시티대학
1996년 미국 콜로라도대학
1997년 ~ 1998년 정보통신정책실 기술심의관
1998년 ~ 2000년 정보통신부 공보관, 국제협력관, 우정국장
2000년 ~ 2001년 정보통신부 전파방송관리국장
2001년 ~ 2005년 부산, 서울체신청장
2005년 ~ 2007년 정보통신부 우정사업본부장
2007년 ~ 현재 : 한국정보보호진흥원장