특집

네트워크 시대의 사회적 위험과 정보보호

민경식(한국정보보호진흥원)

Ⅰ. 서론 : 정보위험사회의 등장

21세기의 시작과 함께 우리 사회는 정보 및 과학기술혁명이라는 역사적 · 구조적 변화의 거대한 물결을 맞이하고 있다. 시시각각 눈부시게 발전하는 정보통신기술의 영향력은 이미 산업기술 및 경제분야를 넘어 일상생활의 전 영역에 급속히 확산되고 있다. 남녀노소를 막론하고 인터넷을 통한 접속과 연결은 빠트릴 수 없는 하루일과가 되고 있다. 또한 우리나라는 세계가 인정하는 IT강국이다. OECD, ITU 등 여러 국제기구는 초고속 인터넷 보급률(가구의 88%), 전자정부 구현(브라운대 평가 2년 연속 1위), IT의 경제기여도 등에서 한국을 세계최고수준으로 인정하고 있다.

한편, 현대사회의 과학기술발전으로 사회가 풍요로워질수록 예측 불가능한 위험이 증가하는 정보위험사회(Information Risk Society)를 지적하는 목소리가 높아지고 있다. 위험사회(Risk Society)란 독일의 사회학자인 울리히 벡(Ulrich Beck)이 제시한 개념으로 위험사회에서 대중들은 과학기술의 무제한적 발전 속에서 풍요를 누리면서도 한편으로는 숱한 사회적 위험에 노출된다. 정보위험사회(Information Risk Society)란 특히 컴퓨터와 네트워크와 같은 정보기술의 발전에 따라 대중들이 많은 혜택을 누리면서도 정보기술에 의해 등장한 다양한 역기능들과 같은 새로운 위험들에 노출되어 있는 사회를 말한다. 유비쿼터스 환경으로의 변화와 웹 2.0, SOA(서비스지향아키텍처) 등 신기술 패러다임의 잇따른 등장은 정부, 기업, 개인들에게 예측 불가능한 위험을 증가시키는 정보위험사회로의 진입을 더욱 촉진하고 있는 상황이다. 곳곳에 산재한 컴퓨터를 시간과 장소에 상관없이 자유롭게 이용함으로써 편리하고 쾌적한 정보이용환경을 구현하게 해주는 유비쿼터스 사회(Ubiquitous Society)는 동시에 예측 불가능한 위험이 곳곳에 산재한 '고도화된 정보위험사회'로의 진입을 의미하게 된다. 고도화되고 복잡해진 정보기술이 사회시스템의 핵심 기반으로 자리 잡게 되고 이러한 기술들 간의 컨버전스가 확대되면서, 특정 기술의 약한 고리에서 발생한 위험이 도미노 현상을 일으켜 전 사회의 위기로 몰아 갈 수 있는 잠재적 가능성이 상존하게 된다.

정보위험사회의 진전은 네트워크와 정보기술 발달의 복잡도와 인류사회의 정보기술에의 의존

성 및 결합도 심화에 기인하고 있다. 정보기술 발달에 의한 복잡도의 증가는 IT 기술 자체의 복잡도(complexity)와 IT 환경의 복잡도의 증가로 구분되는데, IT 기술의 복잡도는 기반 기술의 알고리즘 복잡도 증가, 미디어 컨버전스 및 디바이스 통합 등으로 인한 복잡도 증가를 들 수 있으며, IT 환경의 복잡도는 노드의 증가 및 네트워크 경계의 불투명성 증가 등을 들 수 있다. 특히 MIT 연구결과에 따르면 앞으로 인터넷에 연결될 노드의 수는 1조개가 넘을 것으로 예상되며, 유비쿼터스 환경과 BcN(광대역통합망)에 의해 다양한 개인 모바일 단말기기들이 IP 네트워크에 결합되면 그 복잡도의 증가폭이 엄청날 것으로 예측된다.

특히 새로운 정보기술의 등장과 이러한 디지털 기술들 간의 컨버전스 현상은 정보위험의 예측 불가능성을 높이게 된다. 하루에도 전세계적으로 셀 수 없을 정도로 많은 새로운 정보 상품 및 서비스가 등장하고 있지만 충분한 보안성 검토 없이 출시되거나 이용되기 때문에 대중들은 새로운 정보기술에 의한 예측 불가능한 잠재적 위험에 노출될 수 밖에 없게 된다. 이러한 새로운 기술들 중 유비쿼터스 사회의 근본 핵심기술이라고 할 수 있는 RFID, USN, VoIP, BcN, Wibro, Telematics 등은 다양한 잠재적 리스크들을 내포하고 있다. 전세계적으로 보고된 것만으로도 하루가 멀다 하고 수많은 개인정보침해 사고가 발생하고 있으며, Zero-Day Attack 등에서 볼 수 있는 것처럼 정부, 기업, 개인들은 디지털 환경의 일상화된 정보 위험에 노출되어 있다는 것을 알 수 있다.

이러한 정보위험사회의 심각성을 보여주는 사례들을 살펴보면 먼저 밀레니엄 버그 위험을 들 수 있다. '인류의 재앙'이라고까지 불렸었던 2000년 밀레니엄 버그(Millenium Bug) 위험은 정보기술의 예측 불가능한 잠재적 위험성에 대한 전 인류의 인식을 일깨우는 계기가 되었었다. 2003년 1월 25일 국내에서 발생했던 인터넷 대란 사태는 정보기술의 위험이 현실화됨으로써 사회에 미칠 수 있는 파국적 영향력과 금융거래 중단 및 공장생산주문 마비로 이어지는 네트워크 도미노 현상을 보여줌으로써 정보화 강국으로 알려졌던 우리 사회 도처에 내재한 정보위험의 존재를 각인시켜 주었다. 가장 최근 사례를 들자면, e-Stonia로 불리기까지 했던 인터넷 강국 에스토니아에서 사이버 테러로 2007년 5월 3주간 주요 전자정부 사이트와 은행을 포함하여 대부분의 사회시스템이 심각하게 마비되는 일이 발생하여 전세계적으로 사이버테러의 경각심을 높인 바 있다. 최근 들어 <다이하드 4>를 포함하여 많은 영화들이 사이버테러와 같은 디지털 위험사회의 문제점을 사회적 재앙의 일종으로 본격적으로 다루고 있는 점을 보아도 우리 사회가 이미 심각한 디지털 위험사회로 진입해있음을 간접적으로 느낄 수 있다.

국지적으로 발생하는 자연재해와 같은 위험들과 달리 정보위험사회에서의 위험은 전 사회가 네트워크화 되어 있고, 개방형 구조를 가지고 전세계적으로 연결되어있기 때문에 정보사회 이전의 사회에서는 경험하지 못했던 위험발생 공간의 확장을 일으키게 되며, 어느 한 곳의 네트워크가 흔들리면 전체의 네트워크에 파장을 미치고 우리의 삶 한 부분에 한정되지 않고 삶 전체를 위험에 처하게 만드는 네트워크 도미노 현상을 일으킬 수 있다는 점에서 더욱 심각한 문제라고 할 수 있을 것이다. 복잡계(complexity system) 이론가들은 인터넷이 발달한 사회에서 이런 네트워크 도미노 현상이 발생할 경우 사회 전체에 치

명적인 혼란을 일으킬 수 있다고 경고하고 있다. 특히 정보화가 많이 진행되고 사회의 네트워크화가 더 진전된 국가일수록 정보위험에 의한 피해는 상대적으로 더욱 높다고 할 수 있다. 예를 들어 2003년 슬래머 웜에 의한 인터넷 대란 당시 정보화 인프라 수준이 높았던 한국은 일본의 7배, 중국의 2배에 이르는 피해를 입었다. 사회의 거의 모든 시스템이 디지털화되면서 기존 위험들이 정보위험화하거나 정보위험이 다른 위험들을 촉발 또는 확대시키는 결과를 낳게 된다. 대중들의 거의 모든 거래와 활동이 디지털화되고 인터넷에서 이루어지게 됨에 따라 저작권 침해 위험이나 명예훼손 위험, 개인정보 침해 위험 등 기존 위험들이 주요한 정보 위험의 하나로 부상하고 있다. 이처럼 모든 위험요소들의 기술적 기반이자 네트워크를 디지털 기술이 형성하게 되어 정보 위험은 거의 모든 위험과 위기에 직, 간접적으로 연관될 수밖에 없게 되는 것이다. 2006년 12월, 대만 지진으로 해저케이블이 크게 손상되면서 발생했던 국내 통신, 금융 업무의 마비사태는 전세계가 물리적, 논리적으로 연결되고 네트워크화됨에 따라 일국의 통신망 위험이 어떻게 글로벌 위험으로 확대될 수 있는지를 명확히 보여준 사례라고 할 수 있다.

II. 정보위험사회의 위험의 종류

정보기술에 의해 발생하는 예측 불가능한 정보위험은 글로벌, 국가, 기업, 개인의 전사회적 차원에서 발생한다. 디지털 네트워크 사회에서는 이러한 각각의 차원들이 네트워크를 통해 긴밀하게 다층적으로 결합되어 있으므로 각 차원의 위험들은 서로 간에 영향을 끼칠 수밖에 없다. 예를 들어 미국의 엔론 사태는 한 기업의 디지털 회계 부정으로 인한 위기가 국가 경제 시스템의 위기와 국민들의 정신적 공황상태와 같은 개인적 위기로 이어질 수 있다는 위험성을 보여준 바 있다. 정보위험사회의 위험을 글로벌, 국가, 기업, 개인 차원의 위험들로 구분하여 살펴보면 다음과 같다.

1. 글로벌 정보위험(Global Risk)

일반적으로 고도 정보화 사회 이전의 글로벌 리스크는 환경위험과 핵 위험으로 대표되는데, 환경과 핵발전소 및 핵무기 시스템도 기본적으로 IT와 밀접하게 결합되면서 정보위험의 성격을 가지게 되었다. 특히 핵기술과 IT의 결합은 IT 보안 실패로 인한 전 인류의 위험과 직결될 수 있다는 점에서 그 심각성이 매우 높다고 할 수 있다. 이미 감염시킬 대상의 국적을 따지지 않는 인터넷 웜이나 바이러스는 글로벌 리스크로서 정보위험의 특징을 잘 보여준 바 있다. 인터넷을 통해 전세계가 긴밀하게 연결되고 국가 간 전자상거래(cross-border EC)와 기타 거래 활동들이 빈번해지면서 일국에서 발생한 위험은 여러 국가에게 쉽게 영향을 미치게 된다. 특히 미국에서 발생한 신용카드사의 개인정보 유출 사고의 경우와 같이 다국적 기업의 개인정보 유출과 같은 보안사고로 인해 여러 국가의 국민들이 직접적으로 피해를 입는 사례가 늘어나고 있으며, 최근 많은 해킹 공격들이 특정 국가들을 경유하여 이루어지는 경우가 많아 국가 간 법적 분쟁으로 불거지기도 하는 등 글로벌화된 경제시스템 속에서 정보위험은 국가 간에 주요한 갈등요소로 등장하고 있다.

2. 정부의 정보위험 (National/Governmental Risk)

<다이하드 4>를 포함한 여러 영화들에서 보여주고 있는 것처럼 네트워크화된 국가 기반시설에 대한 사이버테러와 해킹 공격 등으로 인해 정부의 기능이 마비되고 사회적 혼란이 야기될 위험이 높다. 또한 전자정부 시스템의 보안 취약성으로 피해를 입은 국민들이 소송으로 인한 시간적, 금전적 손해를 입을 수도 있으며, 전자정부 시스템에서 발생하는 다양한 위험들을 효과적으로 관리하지 못해 정부에 대한 신뢰에 심각한 손상이 가게 된다면 전체 정부사업의 지속성에도 타격을 입게 될 수 있다. 특히 NEIS나 전자주민증과 같이 프라이버시 침해 우려가 높은 정부 IT 프로젝트의 경우 국민들의 반대 때문에 무산되거나 지체됨으로 인해 세금 낭비와 국민과의 갈등해결을 위한 비용이 발생할 수 있다. 국가적으로는 해킹의 주요 경유지라는 국제적 오명과 보안 무법천지라는 불명예를 안게 되는 피해를 볼 수도 있으며, 국가의 이미지 하락과 국내 IT의 신뢰도 하락으로 인한 정보기술 산업 위축, 국가경쟁력 저하 등과 같은 리스크를 안게 될 수 있다.

3. 기업의 정보위험 (Enterprise/Corporate Risk)

기업의 경우 최근 비즈니스 환경 및 법제도 그리고 IT환경의 변화에 따라 보안위험이 증가하고 있는 상황이다. 먼저 비즈니스 환경의 변화를 살펴보면 실시간 기업 개념에서 볼 수 있는 것처럼 전통적인 의미의 기업 경계가 무너져 확장되고 있으며, 기업 비즈니스에서 정보기술이 차지하는 비중이 높아졌으며, 기업 윤리, 투명경영에 대한 요구와 사회적 책임이 증가하고 있다. 전세계적으로는 프라이버시 라운드와 시큐리티 라운드화가 진행되면서 기업이 일상적인 비즈니스 수행 중 심각한 위험에 노출될 수 있게 되었다. 법제도적으로는 제조물책임법, e-Discovery 등 새로운 법적 요구들과 각종 IT컴플라이언스 요구조건들이 증가하고 있고, 개인정보보호관련 소송 증가 및 법제 강화에 직면하고 있으며, 집단소송제나 징벌적 손해배상 등 소비자들의 권리보호를 위한 강력한 법적 조치들에 대한 도입이 검토되고 저작권 침해 및 개인정보 침해로 인한 기업의 법적 책임이 증대되고 있다. 특히 기업의 경우 최근 강화되고 있는 SOX, HIPAA, GLBA, Basel II 등 IT 컴플라이언스들을 준수하지 못했을 경우 집단소송 등으로 심각한 법적, 경제적 피해와 함께 주가 하락, 벌금 및 규제당국의 직, 간접적인 간섭, 비윤리적 기업이라는 낙인으로 기업 이미지와 신뢰도 하락은 물론 고객 이탈로 인한 기업경쟁력 하락과 비즈니스 기회상실이라는 리스크를 안게 될 수 있다.

4. 개인의 정보위험(Personal Risk)

인터넷 등 정보기술을 통한 개인정보 침해와 명예훼손 등의 역기능은 개인의 정신과 육체에 심각한 리스크를 입힐 수 있다. 온라인에서의 신원도용에 이은 개인정보 도용에 따라 자신도 모르는 사이에 신용불량자로 전락하거나 악성루머 등으로 인해 개인의 이미지가 추락해버릴 수도 있다. 개인정보 유출과 악성 리플로 인한 여중생의 자살사건과 위치추적 기능을 이용한 살인사건 등은 디지털 기술에 의해 개인의 신체적 리스크에까지 심각한 영향을 미칠 수 있음을 보여주고 있다. 이뿐만 아니라, P2P, UCC 사이트 등에 의해 개인의 사소한 부주의나 악의적인 의도 없

이 음악이나 사진과 같은 멀티미디어 파일을 다운로드 받거나 타인의 개인정보가 포함된 파일을 올리게 된 경우, 타인의 개인정보 및 지적재산권을 침해한 범죄자로 전락할 수 있는 위험도 높아지고 있다. 유비쿼터스 사회는 물리적 공간과 디지털 공간이 융합되면서 물리적 공간에 존재하는 사물과 사람에 대한 직접적인 통제가 가능하고, 사이버공간과는 달리 물리적으로 영향을 줄 수 있다. 특히 대표적인 유비쿼터스 서비스라고 할 수 있는 U-의료의 경우 신체와 정보기술의 결합도와 의존도가 높아지면서 정보기술의 취약점과 오류는 직접적으로 개인의 신체적 위험으로 확장될 수 있다.

III. 주요 정보위험의 유형

앞서 정보위험의 대상 차원에서 정보위험을 분류해보았다면, 이제부터는 주요한 정보위험의 유형 몇 가지를 살펴보도록 하겠다.

1. 신기술 및 새로운 서비스 등장에 의한 새로운 리스크 발생

앞서 살펴본 유비쿼터스 주요기술들 이외에도 웹 2.0과 서비스지향아키텍처(SOA), 가상화 기술(Virtualization) 등은 현재 전세계적으로 차세대 주요 정보기술 패러다임으로 자리잡아가고 있지만, 이미 웹 2.0 기술에서는 저작권과 프라이버시 침해 등과 같은 다양한 역기능이 발생하고 있고 SOA와 가상화 기술에서도 다양하고 새로운 보안취약점들이 발견되는 등 예측 불가능한 새로운 정보 위험 요소들이 나타나고 있는 상황이다.

신기술로 인한 위험증가의 사례로 광대역 통합망에 의한 보안위협을 들 수 있다. BcN은 차세대 인터넷 프로토콜인 IPv6 체계를 기반으로 통신망, 방송망 및 인터넷망이 All-IP망으로 통합-연계되어, 언제 어디서나 고속으로 끊김 없이 안전하게 서비스를 제공하는 통합 네트워크망을 말한다. BcN의 기본 특성은 Broadband, Convergence, Ubiquitous, Seamless 등을 들 수 있는데, 이러한 특성들은 각각 편리한 멀티미디어 통신을 가능하게 하는 특성임과 동시에 위험을 발생시키고 증폭시키는 특성이라고 할 수 있다. 예를 들어 광대역성을 의미하는 Broadband는 위험의 고속전파를 가능하게 해주며, 통합을 의미하는 Convergence는 위험대상의 증가 및 통합환경에 따른 새로운 위험의 등장을, Ubiquitous 특성은 위험의 시공간적 편재 및 일상화를, 마지막으로 중단없는 서비스를 의미하는 Seamless 특성은 끊임없는 연속적인 위험에 노출될 수 있음을 의미할 수도 있어 편리함의 증가와 함께 위험 또한 심각하게 커질 수 있다. 또한 유무선 이기종 망간의 표준 API를 통한 통합에 따라 기존에는 폐쇄망으로 운영되어 상대적으로 안전하였던 방송망이나 음성통신망 등의 개별망으로 위험이 확산될 수 있어 이러한 개별망들이나 USN까지 통합망 전체로 피해가 확산될 수 있는 위험이 존재한다. 또한 BcN 기술을 이루고 있는 IPv6, USN, 고성능 무선 디바이스들과 같은 신기술들과 IPTV, VoIP와 같은 서비스들 각각에 대한 충분한 보안성 검토나 종합적 보안대책이 미비한 상황이기 때문에 이러한 기술과 서비스들로 인한 예측불가능한 리스크들이 더욱 증가할 수 있다. BcN은 연결과정에서 위치정보 등 개인정보 수집이 이루어지면서 개인정보 침해 위험이 높아지게 되며, 개인디바이스들

의 고성능화에 따라 개별 디바이스에 대한 공격 등을 통한 침해 가능성이 늘어나게 된다. 또한 개인정보영향평가가 이루어지지 않은 BcN상의 취약한 서비스들로 의해 개인정보위험이 증가되며, 망간, 기업간 연동구간에서 발생 가능한 잠재적 취약점과 위협으로 개인정보 유출가능성이 높아지게 된다.

2. 개인정보 침해, 산업기밀유출 등 데이터 거버넌스 실패 위험

예전의 기업과 정부기관에서의 위험이 주로 내부의 정보시스템에 대한 외부의 공격이고 정보보호의 목표도 외부의 공격으로부터 정보시스템을 투자대비효과(ROI, Return on Investment)의 관점에서 안전하게 지키는 것이었다면, 지금은 외부 공격으로부터 내부 정보시스템을 보호하는 것은 물론이고 기업, 정부, 개인의 데이터가 대부분 디지털화되어 시스템에 저장되면서 데이터의 적절하고 적법한 관리에 대한 사회적, 윤리적 의무와 책임을 준수하는 것으로 확대되었다. 정부와 기업은 개인정보 유출 등의 데이터에 대한 적절한 보호를 제공할 것을 요구하는 법적 컴플라이언스 미준수에 따른 법적 책임이라는 새로운 과제에 직면하고 있다. 데이터 거버넌스(Data Governance)는 산업기밀보호와 소비자 개인정보보호, 법적 증거와 연관된 e-Discovery 의무와 같은 IT 컴플라이언스들을 준수하기 위해 자신이 보유하고 있는 데이터에 대한 관리와 통제를 의미한다. 앞서 살펴본 대로 대부분의 IT 컴플라이언스들에서는 데이터를 보유하고 있는 기업들이 데이터들에 대해 합리적인 수준의 보호를 제공할 것을 의무화하고 있는데, 다양한 컴플라이언스들의 보호 기준을 만족시키기 위한 데이터 거버넌스를 확립하지 못한 기업들은 의무를 준수하지 못했을 경우 엄청난 벌금과 같은 손해를 입거나 이미지 하락 등의 위험을 감수해야 한다.

3. '신뢰(Trust)'의 상실

정보기술에 의한 혹은 정보기술에서의 가장 심각하고 장기적인 위험은 바로 인류의 네트워크 생활공간에서 신뢰(Trust)가 사라지게 되는 것이라고 할 수 있다. 이미 '역사의 종말'의 저자 프랜시스 후쿠야마는 지식정보사회가 지속적으로 성장하기 위해 사회적으로 가장 필요한 자본으로 '신뢰(Trust)'를 꼽고 있다. 비대면적인 디지털 네트워크상에서 개인과 개인 간의 신뢰, 개인과 기업 간의 신뢰, 개인과 정부 간의 신뢰, 국가와 국가 간의 신뢰가 사라질 때 냉각효과에 의해 전자상거래를 포함한 모든 네트워크상의 트랜잭션이 심각하게 위축되고 네트워크 인프라는 무용지물이 되어버리는 회복 불가능한 심각한 위험이 발생할 수 있다. 온라인 네트워크 상에서 신뢰가 사라지고 약해지는 이유는 네트워크 자체가 해킹, 개인정보침해와 같은 보안위험에 취약하기 때문이기도 하지만, 직접적으로 온라인에서의 신뢰 관계를 노리는 공격이 등장했기 때문이다. 'Applied Cryptography'의 저자 브루스 슈나이어는 이러한 공격들을 정보시스템의 취약점을 이용해 정보시스템을 공격하는 기존의 Physical, Syntactic Attack와 구별하여 디지털 정보의 의미를 조작하여 인간의 취약점을 공격하는 제3세대 공격법으로서 Semantic Attack이라고 부르고 있다. 기존의 사회공학(Social Engineering)을 넘어 2000년대 들어 인터넷 상의 사람과 사람 간의 신뢰관계를 이용하여 신뢰

시스템 자체를 직접적으로 공격하는 공격법이라고 할 수 있다. Semantic Attack은 흔히 Cognitive Hacking(인지적 해킹)이라고 부르는데, 인지적 해킹은 디지털 정보를 위변조하여 사람의 심리를 변화시킴으로써 어떤 행동을 하도록 만드는 공격을 말한다. VoIP환경이 도래하면서 IP망을 이용한 피싱과 비싱 등도 넓게 보면 이러한 공격에 포함된다고 할 수 있을 것이다. 직접적이든 간접적이든 온라인 공동체나 디지털 네트워크에 대한 사람들의 신뢰, 기업과 정부, 타인들에 대한 개인들의 신뢰에 대해 이루어지는 공격들은 슈나이어의 말처럼 새로운 제3세대 정보 위험으로 자리잡고 있다.

Ⅳ. 위험관리로의 정보보호 패러다임 전환을 위한 세부 추진과제

1. 신기술에 대한 영향평가 활성화 방안 연구

신기술 및 새로운 서비스에 대한 사전영향평가의 활성화 및 영향평가의 위험관리 도구로서의 실효성을 보장할 수 있는 대책에 대한 연구가 필요하다. 새로운 정보기술이 가져올 예측 불가능한 잠재적 위험이 심각하기 때문에 사전 보안성 검토 및 정보기술영향평가는 사회적 위험관리의 기본적이고 핵심적인 기술이라고 할 수 있다. 정보기술에 대한 적절한 사회적 통제가 이루어져야 하며, 모든 IT 기술은 적절한 사전위험분석을 통한 사회적 합의를 통해 그 사용여부 및 발전 여부가 결정되어야 한다. 현재 개인정보영향평가 제도가 제한적으로 실시되고 있지만 그 수행범위나 법적 근거의 부재와 평가 대상 선정 및 수행방식 등의 문제 때문에 위험관리수단으로서 사전영향평가제도의 실효성이 의문시되고 있는 상황이다. 합의회의제도 등 해외의 영향평가 제도 및 국내 환경영향평가 등 다른 영향평가제도에 대한 벤치마킹을 통해 정보기술영향평가 등 정보기술이 가져올 수 있는 사전위험평가제도들의 효과성을 제고하고 활성화할 수 있는 방안에 대한 연구가 필요하다.

2. 웹 2.0 환경에 맞는 위험관리방법론의 개발

기존의 위험관리는 분산된 자원들과 다양한 위험들에 대해 모니터링하고 발생한 위험들에 대처하기 위해서 관리와 집행을 집중화하는 것이 주요 흐름이었다고 할 수 있다. 하지만, 이러한 중앙 집중적 위험관리는 급변하는 비즈니스 환경과 기술의 변화, 그리고 기하급수적으로 증가하는 접속노드의 증가와 데이터양의 폭발적 증가 및 Semantic Hacking 앞에서는 많은 한계점을 노출하고 있다. 따라서 집중적 위험관리와 함께 이를 보완할 수 있는 분산화된 위험관리들을 활성화시키고 이를 통합할 수 있는 방법론에 대한 연구가 요청된다. 이를 위해서 최근 새롭게 등장한 웹 2.0의 참여, 공유, 개방성이라는 긍정적 특징과 RSS, AJAX와 같은 기술, 그리고 블로그와 소셜네트워크라는 시스템을 정보보호 및 위험관리에 활용할 수 있는 방안에 대한 연구가 필요하다.

3. 사회적 안전망으로서의 공적 정보보호 서비스 제공에 대한 연구

정보화 과정에서 주요 문제점의 하나로 등장했

던 것이 정보격차(Digital Divide)였다면 정보위험사회에서 주요 문제점으로 정보보호격차(Security Divide)가 등장할 수 있다. 기술적, 금전적 이유로 (개인)정보보호 서비스에서 소외되어 위험에 무방비로 노출되는 계층이 등장하는 것을 정보보호격차라고 할 수 있는데, 정부는 위험관리 차원에서 이러한 정보보호격차가 발생하지 않도록 적절한 방안을 마련해야 한다. 정부의 경우, 전반적인 정보보호 산업의 규모와는 상관없이 개인 컴퓨터들의 정보보호 실패로 인해 DDoS 공격의 경유지로 악용됨으로써 국가적 이미지 손실과 국내 IT 제품들에 대한 평가 절하 등의 피해를 당할 수 있으므로, 위험에 적극적으로 대처하여 약한 고리를 제거하기 위한 노력이 경주되어야 한다. 위험관리 차원에서 약한 고리를 최소화하면서 국민들의 정보보호격차를 해소하기 위해 기본적으로 제공되어야 하는 공공재로서의 정보보호 서비스의 수준과 그 효과에 대해서 연구가 이루어져야 할 것이다.

4. 사이버 침해 사고 고지 의무화 도입 검토

효과적인 위험대응을 위해서는 정확한 위험분석이 선행되어야 하는데 이를 위해서는 기존 위험들에 대한 충분한 데이터의 양과 정확도가 필요하다. 하지만 많은 경우 기업들과 기관들은 사고 발생에 대하여 공개하지 않고 무마하고 있기 때문에 유의미한 통계치가 나올 수 있는 사건 수집이 어려울 수 있다. 효과적인 위험관리를 위한 위험분석의 정확성을 보장하고 추가적인 사고를 방지하기 위해 사이버 침해사고 발생 시 기업에게 그 사실을 피해자들에게 고지하도록 의무화하는 제도 도입을 검토해야 한다.

5. 취약점 공개 인센티브 제도 연구

새로운 위험은 시스템과 서비스의 내부 취약점에 대한 외부 위협이 현실화되었을 때 발생하게 되는데, 시스템에 대한 취약점에 대한 정확한 파악도 신속, 정확한 위험분석 및 효과적인 위험관리를 위해 필수적이다. 많은 조직의 경우 자신들의 제품이나 서비스의 취약점에 대해 공개하기를 꺼려하여 보안패치 등 적절한 대응 시기를 놓쳐 버림으로써 많은 사람들을 위험에 처하게 하는 경우가 비일비재하므로, 취약점 공개를 촉진할 수 있는 방안이 모색되어야 한다. 취약점을 발견했을 경우 혹은 취약점에 대한 신속한 자발적 공개 및 조치를 취했을 경우 법적 책임을 경감시키는 등 취약점 제보자나 자발적 취약점 공개 조직에게 인센티브를 줄 수 있는 상벌시스템에 대한 연구가 필요하다. 각 기업이나 조직에 취약점을 신고할 수 있는 공식적인 통로 마련을 의무화하거나 사전에 취약점을 발견하여 공지했을 경우 실제 이러한 취약점을 통한 사고 발생 시 재해복구 및 법적 해결 시 인센티브를 제공할 수 있는 시스템이 고려되어야 한다.

6. 전사회적 신뢰(Trust) 인프라 연구

정보시스템에 대한 신뢰, 정보시스템을 이용하는 개인들 상호간의 신뢰, 정보시스템에 올려져 있는 데이터 내용에 대한 신뢰를 보장할 수 있는 다양한 인프라 기술들에 대한 연구가 필요하다. 또한 정보시스템을 이용하여 조작된 내용을 전파함으로써 사람의 인식에 영향을 주어 결국 특정한 행동을 하게 만드는 인지적 해킹(Cognitive Hacking)과 의미론적 공격(Semantic Attack)에 대한 효과적인 대응기술에 대한 연구

가 필요하다. 인터넷 등의 전자매체들이 진실을 취득하는 주요통로가 되는 상황에서 인지적 해킹/의미론적 공격은 인터넷과 정보기술에 대한 신뢰성을 낮추고 냉각효과를 발생시킬 수 있다. 현존 보안기술들은 대부분 Syntactic Attack이나 Physical Attack에 대한 대응을 목적으로 하고 있으며 Semantic Attack에 대한 효과적인 기술의 개발이 아직은 미진한 상황이다. 디지털 정보 내용의 신뢰성을 제공하기 위한 기술에 대한 연구개발을 통해 사람들이 네트워크상의 잘못된 정보를 가지고 그릇된 행동을 통해 위험에 빠지는 일이 없도록 해야 한다. 특히 수많은 잘못된 정보들 사이에서 신뢰도가 높은 의미 있는 사실들을 밝혀내기 위한 협력필터링과 신뢰성 보고와 같은 방법들이 연구되어야 하며, 이 과정에서 웹 2.0의 기술 및 특징을 이용하는 방법에 대해 연구될 필요가 있다. 데이터의 신뢰도 검증과 조작여부를 밝힐 수 있는 기술을 통해 인터넷을 통해 수많은 사람들이 잘못된 행동을 하는 위험을 걸러낼 수 있는 기술 개발이 시급하다. 특히 디지털화된 기업회계자료 조작 및 주가조작과 같은 경제적, 사회적 파급력이 큰 사건의 경우 기업회계데이터의 조작여부를 밝힘으로써 건전한 경제활동을 유지하게끔 할 수 있게 해주는 신뢰성 높은 디지털 포렌식 회계(Digital Forensic Accounting) 기술의 연구가 필요하다.

7. 위험관리 기술 개발 및 활성화 방안 마련

유비쿼터스 환경에서 도처에 산재한 다양한 디바이스와 정보들에서 발생할 수 있는 위험들을 효과적으로 억제하고 관리할 수 있는 위험관리 기술 관련 연구가 필요하다. 정부, 기업, 개인이 정보위험을 효과적으로 관리할 수 있게 해주는 위험관리기술이 각각 개발되어야 한다. 현재 기업의 효과적인 위험관리를 도와주는 RMS, TMS, SIM, ILM 등 기업용 솔루션들은 존재하지만 개인의 위험을 효과적으로 관리해줄 수 있는 전용 툴은 존재하지 않거나 개발이 미진한 상황이다. 정보기술의 발전에 의해 개인 신체와 정보기술의 결합도가 높아지고 디지털화된 개인정보 침해에 의한 위험이 높아졌음에도 불구하고 개인이 능동적으로 자신의 위험을 관리할 수 있는 기술적인 대책은 부재하다. 개인들이 정보기술에 의해 발생할 수 있는 위험들을 스스로 관리할 수 있는 효과적이고 비용효율적인 기술들이 연구개발 되어야 한다. 이를 위해서는 핵심적 위험관리 도구로서의 디지털 포렌식 기술 개발 지원 및 핵심적인 개인정보 위험관리 기술로서의 프라이버시강화기술(PETs)의 연구개발지원이 필요하다. 디지털 포렌식은 SOX나 HIPAA, e-Discovery 등 다양한 컴플라이언스의 의무를 준수할 수 있게 해줌과 동시에 위험들을 보다 정확하게 진단할 수 있게 해주는 도구로서 조직의 위험관리의 기본적이면서 핵심적인 도구이다. 디지털 포렌식 기술 개발을 위한 지원 및 디지털 포렌식 기술 사용을 활성화하기 위한 법적 환경 조성에 대한 연구가 필요하다. PETs는 최근 가장 심각한 위험으로 대두되고 있는 개인정보침해위험을 관리하기 위한 핵심기술로 각국의 다양한 프라이버시 법제들 및 컴플라이언스를 효과적으로 준수할 수 있게 해준다. PETs에 대한 연구개발 지원 및 활성화를 위한 개인정보보호법안 통과 등 법적 환경이 조성되어야 한다.

8. 국제적 IT 컴플라이언스 대응 환경 조성

각종 개인정보보호 관련법들과 SOX, HIPAA,

GLBA, e-discovery와 같은 국제적 IT 컴플라이언스들은 억지로 지켜야 하는 번거로운 규제가 아니라 예측 불가능한 정보 위험들을 사전에 억제하고 관리할 수 있는 사회적 안전장치이자 위험관리 도구로 인식시키기 위한 교육 및 홍보가 수행되어야 한다. 세계시장에 진출해있는 국내 기업들이 적절한 컴플라이언스 준수 실패로 인해 기업의 국제경쟁력과 국가경쟁력을 잃게 하지 않기 위해 현재 국제적으로 운용중인 수많은 IT 컴플라이언스에 대해 모니터링하고 기업들에게 IT 컴플라이언스 정보와 합리적인 대응방향을 제시해줄 수 있는 국가차원의 '컴플라이언스 정보센터' 운용이 필요하다. 또한 국내 IT 컴플라이언스 관련 법제도 환경이 구축되어야 한다. 우선 국제적인 컴플라이언스와 비교하여 국내 법제도적 위험관리 수준을 평가하고, 국제적으로 요구되는 수준의 국내 IT 컴플라이언스 법제정 및 법 개정 노력이 필요하다. IT 컴플라이언스를 통한 위험관리 활성화를 위해 IT 컴플라이언스 대상 기업들이나 조직들이 컴플라이언스들을 자발적으로 제공하고 준수하지 못했을 경우 사회적 제재를 받을 수 있도록 함으로써 IT 컴플라이언스 준수를 유도할 수 있는 활성화 방안이 검토되어야 한다.

9. 정보위험사회 정보보호 아젠다 개발

정보위험사회의 위험관리에 적합한 새로운 정보보호 아젠다 개발이 필요하다. '따뜻한 유비쿼터스 세상'과 같은 추상성을 뛰어넘어, 인류 공동의 정보 위험에 대한 공동의 문제의식을 제기하고 정부, 기업, 개인의 사회적 책임감과 윤리성, 참여의식을 고취할 수 있는 차세대 정보보호 아젠다가 개발되어야 한다. 이를 위해 글로벌 환경 아젠다인 '지속가능한 개발(sustainable development)'에 대한 벤치마킹 연구가 필요하다. 또한 이렇게 개발된 새로운 위험관리 정보보호 아젠다에 따른 실천을 활성화시키기 위해 다양한 전략이 모색되어야 한다. 예를 들어 다우존스 지속가능성 지수(DJSI)나 사회적 책임에 관한 ISO26000시리즈처럼 아젠다에 따른 기업의 능동적인 실천이 기업의 가치 증진과 경쟁력 향상에 이바지해 긍정적 실천의 선순환을 이루도록 하는 것과 같은 가치평가 제도 개발이 필요하다. 또한 일회성 캠페인이 아니라 새로운 아젠다에 기반을 둔 사회적 정보위험관리 과정에 개인들이 능동적으로 참여할 수 있는 문화운동 조성이 필요한데, 이를 위해서는 환경위기에 대한 '지속가능한 개발' 아젠다 하에서 등장했던 LOHAS (Lifecycle of Health and Sustainability)와 같은 윤리적 생활양식이나 문화운동 사례와 그 동력에 관한 연구 등이 필요하다.

10. 위험관리 시대에 적합한 보안 인력 양성

최근의 위험은 디지털 저작권 문제나 개인정보보호 문제 등 단순히 기술적인 문제로는 해결할 수 없는 복합적인 경우가 많다. 이 때문에 정보보호 위험관리자는 복합적인 문제를 해결할 수 있을만한 능력을 배양해야 한다. 새로운 보안 인력은 급변하는 정보기술 환경과 새롭게 등장하는 IT 기술에 대해 적절하고 합리적인 기술정책을 생산하고 이에 따른 위험을 효과적으로 통제할 수 있는 능력을 갖추고 있어야 한다. 국가와 기업의 리스크에 효과적으로 대처하기 위해서는 기존의 보안기술에 대한 지식뿐만 아니라, 총체적인 시각을 갖추고 지속적으로 리스크를 관리할

수 있는 능력을 갖춘 보안 인력을 확충함으로써 보안 인력의 양뿐만 아니라 새로운 환경에 부합하는 질도 겸비할 수 있는 인적자산 교육 및 운용 정책을 수립해야 한다. 새로운 보안 인력은 다양한 학문적 식견을 갖추고 있어야 하며, 이러한 다양한 학문을 아우르면서 적절한 정책적, 기술적 능력을 갖춘 인재를 양성할 수 있는 교육프로그램이 개발되어야 한다.

또한 조직적 차원에서도 정보위험사회의 통합적 위험관리 조직로서의 정보보호 조직의 변화에 대한 연구가 진행되어야 하며, 기업 및 기관에 효과적인 위험 관리를 위한 CRO(Chief Risk Officer), CCO(Chief Compliance Officer) 등의 도입을 검토할 필요가 있다.

11. 사이버 위험관리를 위한 법제 및 집행 체제 개선

우선 정보위험사회에서 정보위험이 차지하는 중요성을 반영하여 통신비밀보호법, 재난 및 안전관리 기본법 등 관련 법률에 명시적으로 사이버테러와 같은 심각한 사이버 위기를 국가 위기에 포함시켜 핵심적인 국가 위기상황으로 관리되어야 한다. 현재 정보보호 관련 법제들은 개별 법률로의 분산 및 법제간의 충돌로 인해 비효율성이 증가되고 정보보호 관련 집행기구들 또한 분산 및 역할 중첩과 혼선으로 갈등이 증폭되어 효율적인 통합위험관리가 어려운 실정이다. 위기관리 관련법들과 집행체제도 업무의 중복성과 지휘체계의 혼란을 피하고 효과적인 위기관리체제를 달성하기 위해 통합되어야 할 필요가 있다. 현재 정보보호 관련법들은 다양한 개별법들로 분산되어 있으며 집행기구도 분산되어 있는 상황으로, 새로운 리스크들과 국가적 디지털 위기상황에 효과적으로 대응하기 위해서는 정보보호 관련 조항들을 단일법으로 통합함으로써 법적용의 혼선을 줄이고 법집행기구도 단일화함으로써 집행의 효율성을 높여야 한다. 또한 최근 정부/기업/개인의 최대의 리스크 요소로 작용하고 있는 개인정보보호 위험에 효과적으로 대응하기 위해서는 개인정보보호법의 마련이 시급히 요구된다고 할 수 있다.

새로운 위험들과 국가적 디지털 위기상황에 효과적으로 대비하기 위해서 정보보호 통합법 제정을 효과적으로 추진, 집행할 수 있는 정부 내에 독립적인 정보보호 본부가 신설되어야 할 것으로 보인다. 정부가 독립적인 전자정부위원회를 두고 강력한 추진을 통해 전자정부를 성공적으로 발전시켜온 것처럼 정부는 독립적인 정보보호 본부를 설치하고 국가 정보보호 예산에서부터 기획, 집행에 이르는 실제적인 주도권을 제공함으로써 국가의 정보위험관리 의지를 보여주고 효과적인 통합위험관리체계를 마련할 필요가 있다.

V. 결 론

지금 까지 살펴본 바와 같이 현대 정보사회는 위험이 상존하고 있다. 특히 모든 기기와 사물이 네트워크로 연결되는 환경에서는 하나의 시스템의 위협이 전체 사회시스템을 마비시킬 수도 있게 된다. 정보보호 사고는 그 특성상 완전히 차단할 수는 없다. 즉 지금의 사회를 정의하자면 사고전제(事故前提)사회라 할 수 있다. 따라서 위험을 미리 예측하고 대비함으로서 사고 발생으로 인한 피해를 최소화, 즉시복구체제 정비 등 정책적 대응책이 필요할 때이다.

참고문헌

[1] 민경식 외(2008), 『유비쿼터스 환경에서의 정보보호 정책방향』정보통신연구진흥원.
[2] 김현곤 외(2005), 『유비쿼터스사회 신뢰성 확보를 위한 제도 개선방안 연구』한국전산원.
[3] 김성국 외(2005), 『21세기 한국 사회의 구조적 변동』정보통신정책연구원 편, 민음사.
[4] 김용학 외(2005), 『인터넷시대의 사회적 위험』정보통신정책연구원.
[5] 홍성태 외(2005), 『정보위험사회의 도래와 대응에 관한 연구』정보통신정책연구원.

저자소개

민 경 식

1997년 일본 메이지(明治)대학교 경제학석사
2002년 일본 메이지 대학교 경제학박사
1999년 4월~2002년 3월 메이지 대학교 정보교육센터 조수
2002년 6월~2003년 6월 성균관대학교 경제학부 박사후 연구원
2005년 4월~현재 일본 하이퍼네트워크사회연구소 공동연구원
2007년 3월~현재 성균관대학교 정보통신대학원 강사
주관심 분야 : 정보통신경제학, 정보사회, 정보통신정책