방송통신정책연구
09-진흥-라-11

미래 인터넷 환경에서의 선제적 보안정책 연구

(The study of the anticipative information security policy in the future Internet)

2009. 8.

연 구 기 관 : 한국인터넷진흥원(KISA)
연구 책임자 : 이종화(KISA 수석연구원)
참여 연구원 : 정만현(KISA 연구원)
한정화(KISA 연구원)
자 문 위 원 : 김형종(서울여자대학교 교수)
서승우(서울대학교 교수)
오희국(한양대학교 교수)
정익재(서울산업대학교 교수)

제 출 문

방송통신위원회 위원장 귀하

본 보고서를 **『미래 인터넷 환경에서의 선제적 보안정책 연구』**의 연구결과보고서로 제출합니다.

2009. 8.

연 구 기 관 : 한국인터넷진흥원(KISA)
연구 책임자 : 이종화(KISA 수석연구원)
공동 연구원 : 정만현(KISA 연구원)
한정화(KISA 연구원)
자 문 위 원 : 김형종(서울여자대학교 교수)
서승우(서울대학교 교수)
오희국(한양대학교 교수)
정익재(서울산업대학교 교수)

요 약 문

1. 제목

o 미래 인터넷 환경에서의 선제적 보안정책 연구

2. 연구의 목적 및 중요성

o 기존의 인터넷이 제공하지 못했던 다양한 요구조건들을 반영하여 새로운 네트워크 아키텍처를 설계하자는 미래인터넷에 대한 연구가 본격적으로 시작되고 있음

o 현재 정보보호 관련 대책 수립 및 대응이 이루어지고 있으나 효과적인 정보보호 대응을 위해서는 미래인터넷 및 인터넷의 미래전망을 통해 정보보호 이슈를 도출하여 선제적인 정책적 대응 방안 마련이 필요

3. 연구의 구성 및 범위

o 본 연구의 주된 연구 대상은 앞서 살펴본 바와 같이 향후에 전개될 미래인터넷 환경 변화와 그에 따른 사이버 위협 및 역기능과 이에 대한 대응임
  - 이를 대상으로 미래환경변화와 사이버위협을 전망해 보고 이에 대한 대응방안 검토하여 정책적 제언을 도출

o 각국에서의 연구 동향을 분석하고 국내 전문가를 대상으로 향후에 나타날 상황을 전망하여 방안을 마련

o 정보보호 전문가를 대상으로 미래인터넷환경변화와 사이버 위협, 대응 방안에 대한 설문조사를 통해 발현시기와 정책적 우선순위를 도출하고 미래인터넷 환경변화에 따른 사이버 위협과 이에 대한 대응방안을 마련

4. 연구내용 및 결과

o 본 보고서의 전체적인 체계는 다음과 같음

- 제1장: 미래인터넷의 환경분석으로 요구사항의 분석과 개념 정의, 연구의 범위
- 제2장: 각국의 미래인터넷 연구 동향과 보안 연구 동향에 대하여 분석
- 제3장: EU의 보고서를 토대로 인터넷의 미래상과 사이버 위협을 검토
- 제4장: 인터넷의 미래상과 사이버 위협을 토대로 국내 전문가 대상 설문조사 결과를 분석
- 제5장: 연구결과를 바탕으로 정책적 우선순위와 향후 대응방안을 도출

o 본 연구를 통해 나타난 정책적 시사점은 다음과 같음

- 정책적 우선순위는 다양한 ID사용 증가, 웹기반 서비스 경제활성화, 개인정보 경제가치 증가 등의 환경변화에서의 정보보호가 우선시되며, Social Network의 발전, 국가경계 변화, 클라우드 컴퓨팅, 대용량 데이터 집적, Seamless 환경, Internet of Things, 인터넷 속도증가 등의 환경에 대한 정보보호도 서둘러야 할 것으로 나타남
- 대응 방안으로는 사이버 위협별로 악성코드의 예방 및 대응, 해킹 등 사이버 공격으로 부터의 미래인터넷 시스템의 보호, 개인정보보호 강화, 주요기반의 보호, 증가, 개인정보의 유출, 사회공학적 해킹에 대한 대응, 새로운 환경에서의 보안으로 대응방안을 제시

5. 정책적 활용내용

o 미래인터넷에 대한 전문가 대상 조사를 통한 전망으로 정보보호 대응 방안을 검토해 봄으로써 향후 전개될 미래변화에 대응 할 수 있는 정책 수립의 기초자료로 활용 가능

6. 기대효과

o 국외 미래인터넷 관련 연구 동향을 파악해 봄으로써 향후 우리에게 다가올 미래와 사이버 위협을 전망해 보고 정책적 대응 방안 마련에 기여

o 관련 전문가를 통해 미래를 전망해 봄으로써 미래사회에 필요한 보안 위협과 이에 대한 대응, 정책적 우선순위를 검토

o 향후 정부의 정책 뿐만 아니라 관련 연구와 산업계 등 미래인터넷 준비를 위한 기초자료로 활용

목 차

표 목 차

그 림 목 차

Contents

제1장 서 론

제1절 연구의 배경 및 목적

현재 우리는 인터넷 사회라고 할 만큼 인터넷이 우리생활에 깊숙이 파고들고 있다. 단순히 컴퓨터로 정보를 교환하는 수단으로 이용되던 인터넷은 TV로도 전화로도 이용되고 무선인터넷을 활용하여 언제 어디서나 인터넷에 접근하여 다양한 수단으로 이용되고 있다.

이러한 인터넷은 미국의 국방망, 학술망에서 출발했다고 하는 것은 이미 잘 알려져 있는 사실이다. 통신망과 통신망을 연동해 놓은 망의 집합을 의미하는 인터네트워크(internetwork)의 약어인 internet과 구별하기 위해 Internet 또는 INTERNET과 같이 표기하는데, 랜(LAN) 등 소규모 통신망을 상호 접속하는 형태에서 점차 발전하여 현재는 전세계를 망라하는 거대한 통신망의 집합체가 되었다.

인터넷에는 PC 통신처럼 모든 서비스를 제공하는 중심이 되는 호스트 컴퓨터도 없고 이를 관리하는 조직도 없다. 인터넷을 대표하는 조직으로 ISOC(Internet Society)가 있지만 인터넷망을 총괄 관리하는 기구는 아니다. 그러나 인터넷을 총괄적으로 관리하지는 않지만 인터넷상의 어떤 컴퓨터 또는 통신망에 이상이 발생하더라도 통신망 전체에는 영향을 주지 않도록 실제의 관리와 접속은 세계 각지에서 분산적으로 행해지고 있다. 현재 인터넷은 전화망 버금가는 거대한 세계적 정보 기반이 되었으며 통신량은 급속도로 증가하고 있다.

인터넷에서 이용할 수 있는 서비스는 전자우편(e-mail), 원격 컴퓨터 연결(telnet), 파일 전송(FTP), 유즈넷 뉴스(Usenet News), 인터넷 정보 검색(Gopher), 인터넷 대화와 토론(IRC), 전자 게시판(BBS), 하이퍼텍스트 정보 열람(WWW:World Wide Web), 온라인 게임 등 다양하며 동화상이나 음성 데이터를

실시간으로 방송하는 서비스나 비디오 회의 등 새로운 서비스가 차례로 개발되어 이용 가능하게 되었다. 이와 같은 다양한 서비스와 풍부한 정보자원 때문에 인터넷을 정보의 바다라고 한다.

인터넷의 기원은 1969년 미국 국방성의 지원으로 미국의 4개의 대학을 연결하기 위해 구축한 알파넷(ARPANET)이다. 처음에는 군사적 목적으로 구축되었지만 프로토콜로 TCP/IP를 채택하면서 일반인을 위한 알파넷과 군용의 MILNET으로 분리되어 현재의 인터넷 환경의 기반을 갖추었다. 한편 미국 국립과학재단(NSF)도 TCP/IP를 사용하는 NSFNET라고 하는 새로운 통신망을 1986년에 구축하여 운영하기 시작하였다. NSFNET는 전미국 내의 5개소의 슈퍼컴퓨터 센터를 상호 접속하기 위하여 구축되었는데 1987년에는 ARPANET를 대신하여 인터넷의 근간망(backbone network)의 역할을 담당하게 되었다. 이 때문에 인터넷은 본격적으로 자리를 잡게 되었다.

이때부터 인터넷을 상품 광고 및 상거래 매체로 이용하는 상업적 이용 수요가 증가하였으나 정부 지원으로 운영하는 NSFNET는 그 성격상 이용 목적을 교육 연구용으로 제한하고 있었다. 이 때문에 인터넷 사업자들은 따로 협회를 구성하여 1992년 CIX(Commercial Internet Exchange)라고 하는 새로운 근간망을 구축하여 상용 인터넷에 접속하게 되었다.

이러한 인터넷이 우리나라에 들어온 것은 1994년 6월 한국통신이 최초로 인터넷 상용 서비스(KORNET service)를 개시한 이래 많은 수의 인터넷 접속 서비스 제공자(ISP)가 생겨나서 일반인을 대상으로 상용 서비스를 제공하고 있다. 2009년 현재 인터넷이용률은 77.2%이며, 이용자 수는 3,658만명(만3세이상)으로 국민의 77%가 인터넷을 한다고 볼 수가 있겠다.[1)]

1) 방송통신위원회, 2009년 인터넷이용실태조사, 2009. 9.

<그림 1> (만3세이상)인터넷이용률 및 이용자 추이[출처: 방송통신위원회]

그러나 현재의 인터넷은 여러 가지 문제점을 기본적으로 안고 출발하였고, 인터넷이용이 갈수록 증가하고 있어 점차 포화상태에 이르고 있다. 따라서 세계 각국에서는 현재의 인터넷을 뛰어 넘는 다음세대의 미래 인터넷(Future Internet)을 준비하고 있다. 그러나 인터넷의 이용에 있어 가장 중요한 문제는 보안의 문제로 갈수록 개인정보의 이용이 증가하고 콘텐츠의 이용이 증가하고 금전거래 등이 활성화 되면서 정보의 유출은 심각한 사회문제로 부각되고 있다.

보안 위협의 근본적인 문제는 현재 인터넷의 구조적 불완전성에 기인한다. 네트워크 아키텍처, 주소 체계, 라우팅 프로토콜 등 인터넷을 구성하는 핵심 기반 기술들은 효율성을 위해 그 기능을 최소화하여 설계되었다. 인터넷의 보안을 위한 기능들은 새로운 보안 위협이 발생할 때마다 시그너처 및 소프트웨어 패치 등의 형태로 기존의 탐지, 방어 시스템에 추가되어 왔다. 그러나, 이러한 방식의 해결책은 결코 보안 위협에 대한 근본적인 해결 방안이 될 수 없다.

2000년대에 들어서면서 미국을 중심으로 이러한 인터넷의 구조적 문제점을 해

결하기 위한 움직임이 시작되었다. 기존의 인터넷이 제공하지 못했던 다양한 요구조건들을 반영하여 새로운 네트워크 아키텍처를 설계하자는 미래인터넷에 대한 연구가 본격적으로 시작된 것이다. 특히 현재 인터넷이 만족시키지 못하는 미래인터넷의 다양한 보안 요구사항들도 함께 반영하도록 요구 사항들과 핵심 기술들에 대한 연구도 시작되고 있다.

향후 미래사회에 있어서는 이러한 경향이 더욱더 두드러져 미래인터넷을 준비함에 있어 보안의 문제는 필수적인 아젠다라고 할 수 있다. 그러나 아직까지 미래인터넷의 보안문제를 심각히 고려하고 있다고는 할 수 없으며, 향후 우리사회에 있어 가장 민감하고 심각한 문제를 야기하는 보안문제를 검토할 필요가 있겠다.

따라서 본 보고서에서는 미래의 인터넷 환경과 각국에서 준비하는 미래인터넷의 연구동향 및 정보보호에 대한 노력을 분석하여, 미래사회에 나타날 수 있고 심각히 고려해야할 만한 사이버 위협을 도출하여 이에 대한 대응방안을 모색해보고자 한다.

이를 위해 각국에서의 연구 동향을 분석하고 국내 전문가를 대상으로 향후에 나타날 상황을 전망하여 방안을 마련하고자 한다. 본 연구를 통해 이러한 미래사회의 인터넷과 정보보호 환경을 분석하여, 앞으로 다가올 인터넷환경을 안전하게 대비할 수 있도록 사이버 위협에 대한 대응의 정책적 제언을 도출해 보고자 한다.

제2절 연구 범위

1. 미래인터넷과 사이버 위협

미래인터넷이라는 용어 자체에 혼란이 있을 수가 있다. 미래인터넷은 미래에 발전할 수 있는 네트워크 환경을 아우르는 말로 사용될 수도 있고, 현재 미국, 유럽, 한국 등에서 미래인터넷(Future Internet)이라고 지칭하는 특수한 형태의 네트

워크 구조가 될 수도 있다. 본 절과 다음 절에서 언급하는 사이버위협 및 그에 대한 대응방안은 전자의 의미를 가지고 있는 포괄적인 의미의 미래인터넷의 범주에서 다룰 것이며, 국내외 미래인터넷의 보안 연구동향 부분에서는 후자의 의미를 지니고 있는 용어를 사용할 것이다.

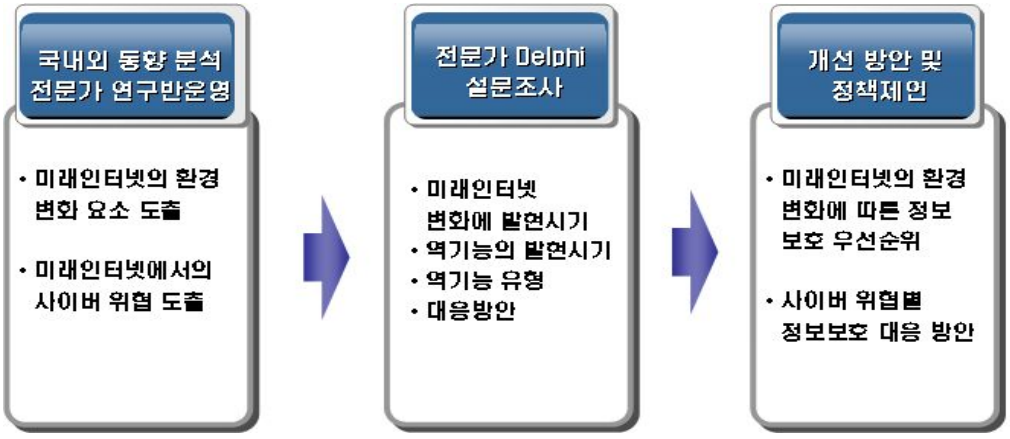
미래인터넷의 사이버위협을 예측하기 전에 미래인터넷이 어떤 형태로 발전될 것인지를 살펴봐야 한다. 미래인터넷이 어떠한 형태로 발전되느냐에 따라 그에 따른 사이버위협 또한 달라질 것이기 때문이다. 미래인터넷이 발전하는 형태는 크게 3가지로 나눠서 생각해볼 수 있다. 첫 번째는 현재인터넷에서 중요한 역할을 하고 있는 전자 상거래와 같은 재정적인 거래가 인터넷을 통해 계속 이루어지거나 혹은 더 큰 역할을 차지하는 형태이다. 이러한 상황에서 가장 큰 문제가 되는 것은 재정적인 이익을 탐해서 악성 코드나 위조 등을 하는 것이다. 즉 악성소프트웨어와 전자 사기가 가장 큰 문제가 될 것이다. 두 번째 형태는 인터넷 연결이 현재의 일반적인 네트워크망 뿐만이 아니라 다양한 모바일 디바이스에서도 이루어지는 스마트 환경의 등장이다. 이로 인해 수많은 유비쿼터스 환경의 작은 기기들 간의 통신에서 생기는 사이버위협이 문제가 될 것이다. 마지막으로 미래인터넷은 중요 기반 시스템을 통제하는 데도 많이 사용될 것이다. 이것은 중요한 인프라나 산업 공장을 제어하는 것을 아우르는 개념이다. 이로 인해 사이버 위협이나 소프트웨어 실패 등은 막대한 경제적 손실 및 인명 피해를 야기할 수 있다. 따라서 미래인터넷은 이러한 모든 형태의 사이버위협에 대응할 수 있어야 한다.

2. 연구 범위 및 분석틀

본 연구의 주된 연구 대상은 앞서 살펴본 바와 같이 향후에 전개될 미래인터넷 환경 변화와 그에 따른 사이버 위협 및 역기능과 이에 대한 대응이다.

본 보고서의 전체적인 체계는 우선 제1장에서는 미래인터넷의 환경분석으로 요구사항의 분석과 개념 정의, 연구의 범위를 다루고 있다.

제2장에서는 각국의 미래인터넷 연구 동향과 보안 연구 동향에 대하여 분석하였다. 제3장에서는 EU의 보고서를 토대로 인터넷의 미래상과 사이버 위협을 검토하였고, 제4장에서는 인터넷의 미래상과 사이버 위협을 토대로 국내 전문가 대상 설문조사 결과를 분석하였다. 제5장에서는 이상의 연구결과를 바탕으로 정책적 우선순위와 향후 대응방안을 도출하였다.



<그림 2> 연구 분석틀

제2장 국내외 미래인터넷 관련 동향

현재의 인터넷은 완전한 전송품질, 신속한 이동성 제공, 완벽한 보안, 확장성, 망 중립성 등의 측면에서 많은 기술적 한계점과 회의가 있어 왔다. 또한 미국, 유럽과 다른 산업 국가에서 미래인터넷의 설계 및 개발 원칙에 관한 연구 개발 시작을 발표하였다. 미래 인터넷이라는 용어에는 상당히 이질적이면서도 상호 연결된 대규모의 네트워크 ICT 인프라가 등장했다는 의미가 담겨있다. 위와 같은 다양한 문제점의 발생으로 이러한 문제점을 보완, 해결하기 위해 미래 인터넷은 점진적인 방법과, Clean-Slate 방법으로 나눌 수 있다. 점진적인 방법은 기존에 우리가 인터넷의 문제를 해결하기 위해 사용해왔던 방식이며 Clean-slate 방식은 새로운 개념과 개선된 성능을 제공하기 위한 급진적인 방식으로 인터넷의 아키텍처부터 새로 설계하는 방식이다. 현재 인터넷의 한계를 벗어나 완전히 새로운 아이디어를 바탕으로 네트워크 아키텍처를 설계하고 test-bed에서의 실험을 통한 아이디어의 검증을 하며 Clean-slate 방식에 의해 아키텍처부터 통신 프로토콜까지 새롭게 설계될 인터넷을 '미래 인터넷'이라고 한다. 미래 인터넷은 상호 연결된 수천 개의 시스템과 네트워크가 통합된 것으로, 반드시 상호 운용 가능한 것은 아니나 알려진 인터페이스로 개방되어 있고 전용 프로토콜과 수 조개의 다양한 네트워크 컴퓨터, 통신 및 저장 장치를 갖추고 있다. 그러므로 새로운 보안 아키텍처, 모델 및 프레임워크에서 발생할 수 있는 취약성과 위협을 다루어야 한다. 다음은 미국, EU, 일본 등 국외의 미래 인터넷 관련 동향과 보안에 관한 R&D 대하여 조사하였다.

제1절 주요국의 미래인터넷 추진 동향

1. 미국

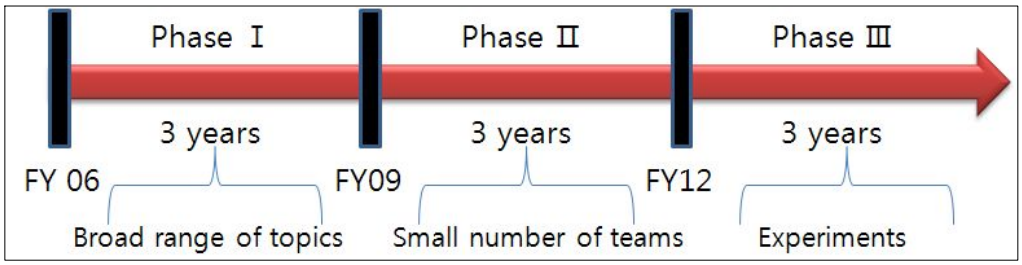
가. 개요

미래인터넷에 대한 연구는 미국을 중심으로 활발하게 진행되고 있다. 미국에는 인터넷의 기반을 이루는 TCP/IP 프로토콜, 라우팅, 네트워크 아키텍처, 보안 등의 핵심 기술들이 충분히 축적되어 있고, 대학 및 기업 연구소를 중심으로 다양한 실험 S/W 및 테스트베드 등의 인프라도 잘 구축되어 있다. 따라서 자금까지 미래인터넷 기술 개발에 있어서 우수한 연구 성과를 보이고 있으며, 다른 후발 국가들에게 훌륭한 롤 모델이 되고 있다. 2000년 DARPA에서 주관한 NewArch 프로젝트를 시작으로 2001년 NSF[2]의 100x100 Clean Slate 프로젝트, 그리고 현재 진행되고 있는 FIND 및 GENI 프로젝트 등이 미국의 미래인터넷 연구를 지원하고 있다.

FIND는 NSF 주관 하에 진행하고 있는 차세대 네트워킹 프로젝트인 NeTS 에 속한 프로그램으로 Prowin, WN, NOSS, NBD와 함께 진행 중이다. FIND의 특징은 미래인터넷을 위한 혁신적인 핵심 기술 및 패러다임을 제안하는 것으로, 2006년에는 총 26개의 개별 프로젝트 형태로 프로젝트 각각 3년간의 기간으로 진행되어, 2009년 현재 42개 과제가 수행중이다. 아직까지 전체 미래인터넷 구조에 대한 연구보다는 Clean Slate 접근방법에 따른 개별적인(bottom-up) 선행 핵심연구에 중점을 두고 있다. 이러한 개별 연구가 큰 성과를 거두고 나면 미래인터넷을 위한 프레임워크와 전체 구조에 대한 연구가 진행될 수 있을 것이다. FIND 프로젝트의 전체 과제규모는 연평균 $11.5M 이다.

---

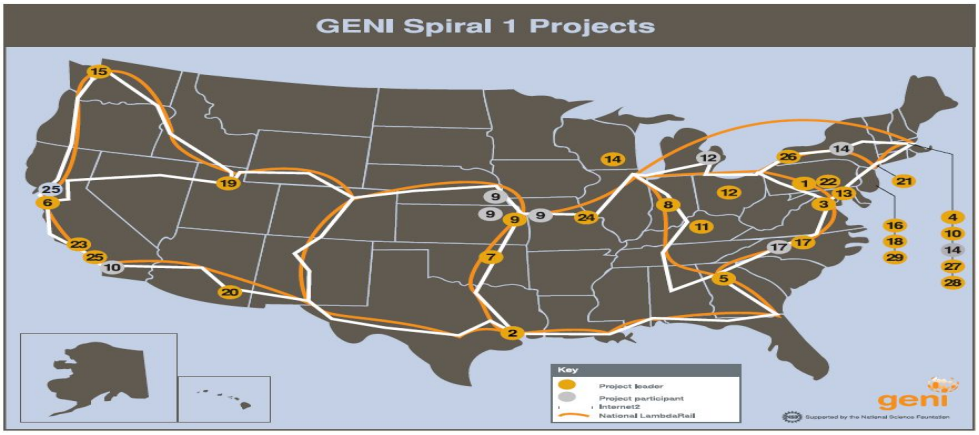
2) National Science Foundation



<그림 3> FIND 진행 상황

출처: http://www.nsf.gov/cise/funding/2007_12_net_sci_eng.jsp, National Science Foundation

NSF는 미래인터넷 연구를 위해서는 다양한 새로운 네트워크 아키텍처들을 동시에, 대규모의 실증적 테스트베드가 필요하다고 보고, 미래인터넷 테스트베드인 GENI의 설계를 2005년부터 시작하여 개념설계안을 완성하였고, 2008년부터 프로토타이핑 과제를 시작 하였다. GENI는 2013년까지 8년간 약 $365M의 예산을 투입하기로 되어있으며, NSF가 중심으로 미국 내 학계, 연구소, 산업체 뿐만 아니라 세계 각국의 기관을 참여시켜서 기존의 인터넷을 뛰어넘는 혁신적인 인터넷 구조를 제시하고 연구, 개발된 기술을 시험 인프라를 이용한 검증을 거쳐 실제망에 도입되도록 하는 목표를 가지고 있다. 이는 PlanetLab의 개념을 확장하여 GENI의 모든 자원들의 가상화와 프로그램-가능 기능을 전 계층에 거쳐 가능하도록 설계될 예정이다.



<그림 4> GENI Spiral 1 구성 MAP

출처: http://www.geni.net

나. 미국의 미래 인터넷 보안 연구

1) FIND 프로그램

미국의 국가과학재단 (NSF)이 주관하는 FIND (Future Internet Design) 프로그램은 현재 미국의 미래인터넷 기반 기술 연구에 있어서 가장 핵심이 되는 프로젝트이다. FIND는 지금부터 15년 후 글로벌 네트워크를 위한 요구조건을 고려하여, 네트워크 아키텍처, 원리, 기술 설계 등 넓은 영역에 걸친 다양한 연구를 수행하는 대규모의 프로그램이다. 2007년부터 시작되어 매년 새로운 주제의 세부 과제를 공모해 왔으며, 현재는 약 40여개의 세부 과제들을 포함하고 있다.

현재 FIND 프로그램에서 수행되고 있는 세부 과제들 중 많은 연구들이 미래 인터넷의 보안 문제를 다루고 있다. 이들은 현재 인터넷의 보안 위협들을 방어하기 위해 다양한 해결 방안들을 제안하고 있다. 이들 중 일부는 앞장에서 제안한 미래인터넷의 핵심 보안 요소기술을 직접적으로 연구하고 있다. 표 1은 현재 FIND 프로그램에서 이루어지고 있는 미래 인터넷의 보안과 관련된 세부 과제들을 앞서 언급한 세 가지 보안 요구사항에 따라 분류하여 나타내고 있다. 비록 제안하는 방법은 각기 다르지만 이들은 한 가지 공통된 특징을 가지고 있다. 기존의 보안 연구들과는 달리, 인터넷 아키텍처 자체를 재설계하거나 혹은 라우팅 프로토콜, IP 주소 등 네트워크를 구성하는 기반 기술을 개선하여 보안 요구사항을 만족시키려 한다는 점이다. 각 과제들의 연구목적과 제안하는 핵심 기술에 대해 간략하게 소개하겠다.

<표 3> FIND 프로그램의 보안 과제

세부 과제	보안 요구사항
CABO: Concurrent Architectures are Better Than One	가용성
An Internet Architecture for User-Controlled Routes	가용성
Designing Secure Networks from the Ground-Up	추적성
Privacy-Preserving Attribution and Provenance	추적성, 프라이버시 보호
Protecting User Privacy in a Network with Ubiquitous Computing Devices	프라이버시 보호

① CABO: Concurrent Architectures are Better Than One

이 과제의 기본 개념은 네트워크 가상화를 통해 기존의 통합된 네트워크 제공자의 역할을 물리적인 네트워크를 제공하는 인프라 제공자 (Infrastructure provider)와 임대받은 네트워크 위에서 다양한 서비스를 제공하는 서비스 제공자 (Service provider)로 분리하는 것이다. 제안하는 CABO 네트워크는 하나의 네트워크 위에 여러 개의 가상 네트워크를 구축함으로써 보안에 따라 차등화된 서비스를 제공할 수 있도록 한다. 예를 들어, 한 가상 네트워크는 강력한 보안 수준을 보장하지만 모든 노드로의 도달성(Reachability)을 제공하지는 못한다. 반면, 또 다른 가상 네트워크는 다른 모든 노드와 통신은 가능하지만 강력한 보안을 보장하지는 못하도록 설계할 수 있다. 다시 말해 앞장에서 언급한 가상화 기술을 이용해 네트워크를 효율적으로 운영하고 가용성을 최대한 보장할 수 있도록 네트워크를 설계하고자 하고 있다. 현재 VINI 테스트베드 위에서 CABO 네트워크를 구축했으며, 다양한 실험을 통해 제안한 네트워크의 성능을 분석하고 있다.

② An Internet Architecture for User-Controlled Routes

이 과제에서는 인터넷 사용자가 데이터를 전송할 경로를 직접 선택할 수 있는 사용자 제어 라우팅 프로토콜을 개발한다. 사용자 제어 라우팅은 경로의 다양성을 통해 단대단 (end-to-end) 성능을 향상시키고 네트워크 가용성을 증대시키며, 간접적으로는 ISP 업체들 사이의 경쟁을 유발하여 서비스의 질을 향상시킬 수 있다. 하지만 사용자에게 더 많은 권한이 부여되었을 때, 이것이 악의적인 목적으로 사용될 경우 더 큰 보안 위협을 초래할 수 있다. 그러므로 이를 방지하기 위한 보안 정책 등을 동시에 고려하고 있다.

③ Designing Secure Networks from the Ground-Up

오늘날 인터넷에서 IP 주소는 악의적인 사용자에 의해 쉽게 변조(spoofing)가 가능하기 때문에, 보안 정책 혹은 경로 제어에 사용되기에 신뢰도가 떨어진다. 네트워크의 보안을 강화하기 위해서는 데이터 트래픽에 그 출처와 의도를 명확히

기술하여 전송되도록 해야 한다. 이 과제에서는 철저하게 보안이 강조된 사설 네트워크인 SANE(Security Architecture for Networked Enterprises)을 제안한다. SANE에서는 사용자가 오직 명백한 허가를 받은 엔드 호스트에 대해서만 접속 권한을 갖는다. 또한 SANE을 구성하는 모든 사용자, 엔드 호스트, 스위치는 오직 이웃 노드로 데이터를 전달하는 데에 필요한 정보만을 갖는다. SANE의 모든 통신은 도메인 컨트롤러에 의해 철저하게 통제된다. 도메인 컨트롤러는 모든 보안 정책 및 경로 정보를 관리하고, 각 사용자에게 데이터 전송의 권한을 부여한다. 현재 SANE은 Stanford 대학과 Wisconsin 대학의 연구소에서 프로토타입이 개발되고 있고, 공공 네트워크(public network)에서의 보안 아키텍처인 InSANE도 연구중에 있다.

④ Privacy-Preserving Attribution and Provenance

이 과제의 목적은 네트워크의 추적성과 사용자의 프라이버시를 동시에 보호하기 위해 속성(attribution)과 출처(provenance)를 지원하는 미래인터넷의 새로운 보안 아키텍처를 개발하는 것이다. 이 보안 매커니즘은 각 네트워크 구성 요소들에게 패킷의 출처와 신뢰성을 결정하는 권한을 부여함으로써 데이터 추적 및 탐지를 용이하게 하고, 한편으로 비밀키 공유를 통해 전송자의 프라이버시 또한 보호할 수 있게 한다. 기존의 IP 프로토콜을 수정하여 출발지 정보를 헤더에 포함시키고 이를 비밀키를 이용해 암호화 함으로써 앞장에서 언급한 보안 요소기술 중 추적성과 프라이버시 보호를 위한 요소기술을 동시에 구현할 수 있도록 하고 있다.

⑤ Protecting User Privacy in a Network with Ubiquitous Computing Devices

전통적으로 프라이버시는 메시지의 기밀성과 동일시되어 생각되었다. 즉, 송신자와 수신자를 제외한 그 누구도 메시지의 내용에 접근할 수 없도록 하는 것이 프라이버시를 제공하는 방법이었다. 지금껏 많은 연구들이 프라이버시를 제공하기 위한 단대단 혹은 링크 계층의 메시지 암호화 프로토콜 개발에 집중해 왔으며, IPSEC, SSL, WEP/WPA 등의 프로토콜은 이미 널리 사용되고 있다. 하지만 유비

퀴터스 컴퓨팅 디바이스들의 등장은 기존의 메시지 암호화를 통한 프라이버시 보호를 더 이상 불가능하게 만들고 있다. 모빌리티, 무선, 임베디드 시스템 사용, 매체의 다각화, 스케일링 문제 등 유비쿼터스 환경의 주요 특징들이 프라이버시 위험을 증가시키고 있다. 이 과제에서는 유비쿼터스 환경의 주요 특징들을 감안하여 사용자의 중요한 정보가 오직 신뢰할 수 있는 사용자에게만 보여질 수 있도록, 네트워크에서 사용되는 이름, 주소와 그것들을 사용하기 위한 메커니즘을 재설계한다.

2) GENI 테스트 베드 보안

GENI 보안과 "인터넷" 보안이 어떻게 다른지를 살펴보는 것은 의미 있는 일이다. 이론적으로, GENI와 인터넷은 다양한 프로토콜을 사용하거나 로컬 또는 원격 운영자가 다양한 프로토콜을 사용하도록 구성한 요소(예: 종단 시스템과 네트워크 장비, a.k.a. 박스)로 구축되어 있다고 간주된다. 이러한 수준의 추상화에서 가장 필수적인 사항은 개별 운영자를 인증하고 다양한 명령과 구성 변경에 대한 권한을 부여하는 수단이고, 보안 ARP, 보안 라우팅, 보안 명명, 보안 전송, 보안 QoS 등 각 고유 프로토콜 계층 내에서 강력한 보안 기능을 통합하는 것이다. 이러한 관점에서 보면, 인터넷의 보안 문제는 기존 인터넷의 사용자 지정 구성, 배포된 프로토콜, 설치 기반과의 하위 호환성을 유지하려는 과정에서 발생한다. 보안 환경에서 네트워크를 배포하는 경우 모든 작업을 안전하게 수행하고 점검할 수 있다. 따라서 GENI에서 새로운 네트워크를 배포할 경우 필수 인증, 권한 부여 및 보안 프로토콜 등을 고려하여 설계해야 하며 최적의 신뢰성 있는 시스템을 갖출 수 있도록 해야 한다.

GENI는 실험 슬라이스 내에서 새로운 네트워크 아키텍처를 구축할 수 있는 가능성을 제공하는 한편, 인터넷 프로토콜에 상당히 의존하는 클리어링하우스, 제어 프레임워크, 구성 관리자, 슬라이스 및 관리 기관을 이용하여 스스로 안전한 환경을 구성할 수 있다. 따라서, GENI는 인터넷 아키텍처에 항상 연결되어 있지 않으며 GENI 보안 기능은 인터넷에서 생성된 비보안 상태를 고려해야 한다(암호화된 VPN 터널에서 GENI를 배포할 수는 있으나 사용자 실험을 수행하기는 힘들

수 있다. 게다가, 최신 네트워크 보안만으로는 프로토콜과 상호 인증 및 권한부여 기술을 구축하고 배포하며 최소 비용으로 신뢰성 있는 GENI 에코시스템을 실행하기가 어렵다. 예를 들면, 기업 및 정부 PKI와 인증된 ID 발급은 비용이 많이 들고 유지하기가 쉽지 않다.

또한 GENI의 주요 전략은 통합을 통한 성장 즉, 기존 설비를 전체 GENI 에코시스템에 통합하고 새로운 기술이 나타나면 이 기술을 추가하며 초기에는 단일 기술을 수용하지 않고 GENI가 주변 상황에 민첩하게 대응하도록 하는 것이다. 그러나 이러한 환경에서 보안 속성을 적용하는 것이 어렵고 특히 요청자와 리소스를 다른 기관에서 관리하고 있으며 다른 권한부여 메커니즘을 갖고 있기 때문에, 이상의 전략은 사용자와 네트워크 운영자의 보안에 관한 높은 관심을 유발하게 된다.

GENI 네트워크 보안 제공 시 가장 다루기 힘든 부분은 권한부여를 위한 인증을 지원하는 것이다. 권한부여 여부를 결정하려면 요청 엔터티에 대한 인증 과정이 필요하다. 보통, 인증 시에는 암호화 기법을 사용한다. 그러나 GENI 네트워크 환경에 기존 암호화 기법을 적용할 경우 특정한 문제에 직면하게 된다. 인증 및 권한부여와 관련하여 GENI 네트워크의 요구사항과 문제점을 검토한다. 그리고 이러한 환경의 주요 위험요소를 살펴보고 현재의 제어 프레임워크를 바탕으로 관련 문제를 해결할 수 있는 솔루션을 제안한다. 또한 경험을 통해 확보한 보안 아키텍처와 대규모 GENI 아키텍처를 지원할 때의 보안 아키텍처를 지원하는 메커니즘의 통합 방법에 연구한다.

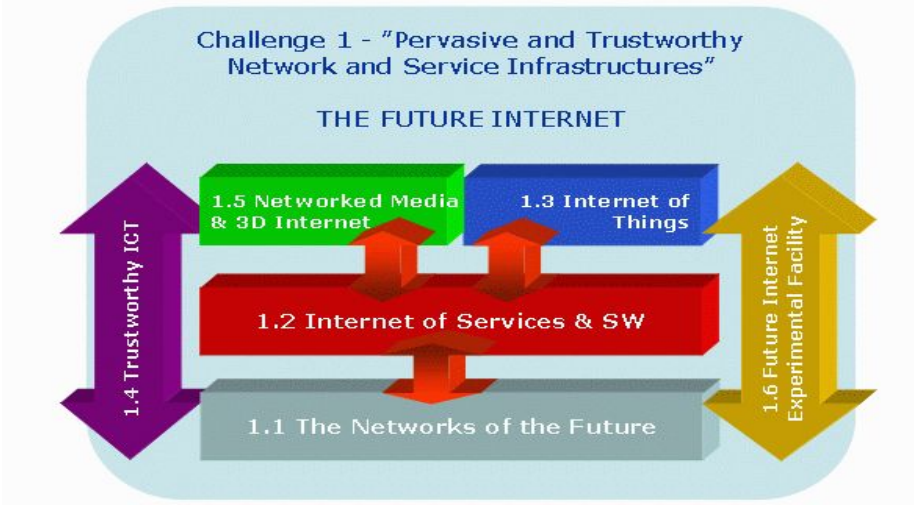
2. 유럽

가. 개요

유럽연합은 1990년대에 접어들면서 미국과의 경제 격차가 점차 확대되자 미국을 따라잡기 위해 리스본 전략을 채택하였다. 이 전략의 목표는 유럽의 정보화를 통한 성장, 고용, 사회적 참여로 요약할 수 있다. 리스본 전략에서 제시된 정보화 모토는 정책과 연구개발을 2개의 기둥으로 하고, 이 두 영역간의 긴밀한 상호협조

를 통해 유럽정보화의 시너지를 창출하자는 것이었다. 정책 부문은 리스본 전략에서 출발하여 신 리스본 전략, i2010 전략으로 발전되어 왔으며, 이에 맞추어 연구개발 부문은 FP5, FP6으로 발전되어 오다가 현재는 FP7이 시행되고 있다. FP7 ICT 연구프로그램은 유럽이 차세대 ICT 및 그 사용에 있어서 세계 선도 그룹에 들기 위해 극복해야 할 7가지 도전과제를 제안하고 있다. 이들 도전 과제들은 크게 업계의 기술 목표 및 사회경제적 목표 달성을 위한 과제로 이분할 수 있으며, 향후 10년 간의 목표와 성과물을 제시하고 있다.

현재 FP7은 2013년 까지 진행 중이며 FP7의 4대 핵심 목표로는 협력(Cooperation), 창의(Ideas), 인력(People), 역량(Capacities) 개발이다. 이를 위해 보건, 식품/바이오/농업, 정보통신, 나노기술, 에너지, 환경, 교통, 사회경제, 안전 및 우주항공 분야 등 9대 핵심 연구 분야를 선정하고 있다. 여기서 미래인터넷은 2007년부터 진행된 FP7내 정보통신분야의 ICT 프로그램에서 관련 연구를 진행하고 있으며 ICT의 7개의 과제 중 첫 번째 과제인 Challenge 1-"Pervasive and Trustworthy Network and Service Infrastructures" 에서 미래 인터넷관련 연구를 진행하고 있다. Challenge 1은 6개의 세부과제로 나누어지며 아래와 그림의 연구영역으로 구성된다. 특히 1.4 과제는 보안 관련 과제이다.



<그림 5> EU, FP7중 첫 번째 과제

출처: http://cordis.europa.eu/fp7/ict/programme/challenge1_en.html

유럽의 미래인터넷 과제는 학교 및 국가연구소외에도 Nokia, Ericsson, Alcatel-Lucent 등의 기업들도 활발히 참여한다. 그리고 네트워킹 테스트베드에 관한 EU의 연구를 통합하기 위한 프로그램으로 FIRE(Future Internet Research and Experimentation)를 진행 중이다.

나. 유럽의 미래 인터넷 보안

유럽은 새로운 보안 아키텍처, 모델 및 프레임워크에서는 미래 인터넷에서 발생할 수 있는 취약성과 위협을 다루어야 하고, 보안 정책은 여러 국가와 관리 도메인, 다른 법규를 준수하거나 고유의 보안 정책을 갖고 있는 다양한 관계자들과 관련된 인프라, 복합 애플리케이션, 가상 엔터티 보호에 적합해야 한다는 목표아래 FP7의 Challenge 1-"Pervasive and Trustworthy Network and Service Infrastructures" 과제에서 다음과 같은 목표를 가지고 프로젝트를 추진 중이며 Euro-NF에 지원을 하고 JRA(Joint Research Activities) workpackage 중 JRA 3.4 (Trust, Privacy and Security)을 통해 미래인터넷을 위한 보안 문제를 다루고 있다.

• 워킹 그룹을 결성하여 모범 사례, 프로세스 및 우선순위를 검토하고 유럽에서 수행할 연구 주제를 선정하며 새로운 연구 분야와 처리해야 할 위협을 파악한다.

• 위협 양상의 변화와 최신 위협 탐지 및 방지 기술을 정기적으로 검토하고 이에 접속할 수 있는 온라인 플랫폼을 구축한다.

• 새로운 위협의 양상과 이러한 위협에 대한 연구를 검토하고 제시하며 업계와 정부가 파트너십을 통해 취해야 할 조치에 대한 조언을 하기 위해, 업계와 학계의 전문가 그룹 및 정책 입안자와 함께 워크숍을 개최한다.

• 개별 워킹 그룹의 연구결과를 활용하여 공격자들이 복합적인 공격으로 보안을 위협하고 유럽연합 사람들의 생활을 파괴하는 내용의 시나리오를 작성한다.

JRA 3.4는 프라이버시(privacy), 무결성(integrity), 인증(authentication), ID보호(identity protection), 서명(signature), 위임(authorization), 키분배(key agreement/distribution), 유효성(validation), 타임스탬프(time-stamping), 증명(witnessing), 익명성(anonymity), 부인봉쇄(non-repudiation), 신뢰성(reliability), 가용성(availability) 등의 보안 서비스를 달성할 수 있는 방법에 대해 연구하는 것이다. 이를 위해 다음과 같이 4단계로 나누어 연구를 진행한다.

Task 1: Lessons Learned from the existing Internet security paradigm

Task 2: Security, Privacy, Availability and Trust Challenges of the Future Internet

Task 3: State of the art report on Future Internet security

Task 4: Future Internet Security Architecture

먼저 현재 인터넷의 보안 메커니즘, 프로토콜, 아키텍처를 분석하여 기존의 보안 문제들을 파악한다. 다음으로 미래인터넷의 서비스 아키텍처에 적합한 새로운 보안 요구조건들을 정의하고 이를 통해 미래 인터넷을 위한 보안 아키텍처를 설계한다. 이 때 보안 아키텍처 설계는 또다시 다음과 같은 세 분야로 나뉘어 연구가 진행된다.

Sub-Task 4.1 Network Security and Privacy Services

Sub-Task 4.2 Network Protection and Availability Services

Sub-Task 4.3 Trust Services

1) 미래인터넷의 환경 분석

미래 인터넷에서는 현재보다 비즈니스 영역의 표준과 규정에 대한 보안 및 신뢰성 요구사항이 점점 복잡해지고 있는 상황에 대처와 고객에게 보증된 서비스 제공을 위한 과제

2) 인터넷의 장기적인 개인정보보호

인터넷에서는 점점 더 많은 개인 정보가 교환되며 저장되고 있으나 사용자의 개인정보는 충분히 보호받지 못하고 있다. 사용자가 개인 정보를 통제하면서 미래 네트워크와 서비스에 대해 ID를 관리하고 지속적으로 개인정보를 보호하는 것을 목표로 하는 통합 프로젝트

3) 개인정보 서비스의 보안 관리

점점 전산화되고 있는 오늘날의 사회에서 사용자는 개인 정보를 제대로 통제하지 못한 채 제3의 기관(예: 병원)에서 이러한 정보를 이용하고 있기 때문에 더욱더 신뢰성 있는 서비스 플랫폼의 개발이 필요하다

그렇기 때문에 신뢰성 있는 서비스를 실행하는 아키텍처를 개발하고 구현하여 분산된 개인정보를 관리하고 처리한다. 이 아키텍처는 신뢰성 있고 강력하며 효과적이고 안정적이다. 처리되고 관리되는 개인정보는 사람들이 참고하거나 보유하고 있는 모든 유형의 정보로 구성할 수 있다.

4) 신뢰성 있는 임베디드 컴퓨팅(Trusted Embedded Computing)

TC(Trusted Computing)는 PC의 무결성과 보안을 검증하고 구현하기 위해 구축한 기술이다. PC에는 사용 가능한 코드 공간, 특정 버스 인터페이스 및 컴퓨팅 전원 등 대규모 리소스가 존재한다. 리소스를 사용할 수 없는 임베디드 컴퓨팅 플랫폼에서는 PC와 유사한 신뢰성 및 보안 문제가 발생한다. 이러한 문제가 발생하는 이유는 플랫폼의 운영 체제와 애플리케이션이 불안정하고 복잡성이 증대되어, 인터넷 연결 시 추가 보안 위협과 공격에 노출되기 때문이다. 제품 및 해당 분야에서 임베디드 컴퓨팅 플랫폼이 PC보다 더 많이 존재하므로 현재 TC(Trusted Computing) 보안 표준을 임베디드 컴퓨팅 플랫폼에 적용할 필요가 있다.

5) 소프트웨어 서비스의 보안 속성 검증

미래 네트워크 인프라에서 소프트웨어 서비스를 동적으로 구성하는 경우 많은 신뢰성 및 보안 문제가 발생할 수 있다. 서비스의 신뢰성과 보안 속성 및 보안 서비스 아키텍처의 동적 구성을 정의하기 위한 최초의 컴퓨터 언어를 개발한다. 이 언어는 속성 검증을 위해 알고리즘과 도구를 갖춘 새로운 소프트웨어 플랫폼에 통합된다.

6) 개인 영역 네트워크(PAN) 및 무선 센서 보안 네트워크

확장 가능하고 신뢰성 있는 보안 네트워킹 프로토콜 스택을 구현하고 검증하며 다중 관리 도메인 및 다른 유형의 애드혹 PAN(Personal Aala Network)과 무선 센서 네트워크의 불안정한 인프라를 통해 데이터 및 서비스의 자동 구성과 보안 로밍을 제공하는 것을 목표로 한다.

7) 다른 유형의, 복원력이 있고, 보안성이 있으며, 복잡하고, 상호 운용 가능한 네트워크 인프라

다른 유형의 네트워크 및 인프라를 보호하여 보안 분야에서 유럽의 잠재력을 강화하는 것에 목표를 두고 있다. 이 프로젝트는 상호 운용 가능한 네트워크 공급자 간 교차 취약성에 초점을 맞추고 있다.

통신 네트워크와 시스템이 점점 복잡해지고 다른 유형이 등장함에 따라 취약성의 정도도 증가하고 있다. 따라서 주요 시스템에서 생성된 제어 정보를 종단 간에 안전하게 전송하려면 네트워크 인프라를 공격과 장애로부터 철저하게 보호하는 것이 필수적이다. 네트워크 시스템 보안을 위해 조율된 전략 및 다수 운영자의 상호운용가능성 향상과 관련된 표준화를 다룬다. 또한 네트워크 인프라 및 시스템의 평가와 인증을 위한 보안 메트릭을 정의한다.

8) 커뮤니티 서비스에 대한 개인정보보호 및 ID 관리

현재 유럽의 다수 사용자들은 소셜 네트워크와 같은 온라인 커뮤니티나 회원 활동을 지원하기 위해 온라인 서비스를 이용하는 실제 커뮤니티에서 작업을 하거나 여가 시간을 보낸다. 또한 유선 통신을 사용하는 커뮤니티뿐만 아니라 모바일 통신 기반의 커뮤니티에도 참여하고 있다. 모바일 커뮤니티에서는 서비스에 대한 강력한 링크를 제공하기 때문에 가상 커뮤니티와 실제 커뮤니티간의 통합이 이루어질 수 있다. 위치 정보와 같은 컨텍스트 정보는 실제 세계의 협력과 자발적인 사회화의 측면에서 중요한 의미를 갖는다. 그러나 사용자가 이러한 커뮤니티에 참여하는 경우 자신도 모르게 개인정보를 제공하게 된다. 그리고 커뮤니티 서비스 제공자는 규정을 준수하고 사용자의 요구에 맞는 신뢰성과 개인정보보호를 제공해야 한다. 또한 커뮤니티 서비스에 대한 자금을 조달하려면 인프라는 스폰서/광고주의 마케팅 활동에 개방적이어야 한다. 통신 서비스 제공자가 제공하는 새로운 커뮤니티 지원 서비스는 상호 운용 가능해야 하기 때문에, 이 때 통신 서비스 제공자 간에 상호운용 가능한 TE(Trust Enablement) 및 개인정보보호를 고려한 새로운 ID 관리 방법이 필요하다.

9) 침해 행위와 공격 위협에 대한 전 세계적인 감시

인터넷 경제와 네트워크 사용자를 공격하는 기존 및 새로운 위협을 파악하기 위한 수단을 제공하는 목표에 도달하기 위해 다음과 같은 세 가지 주요 목적을 설정하고 있다.

① 다양한 보안 관련 원천 데이터(Raw Data)의 실시간 수집

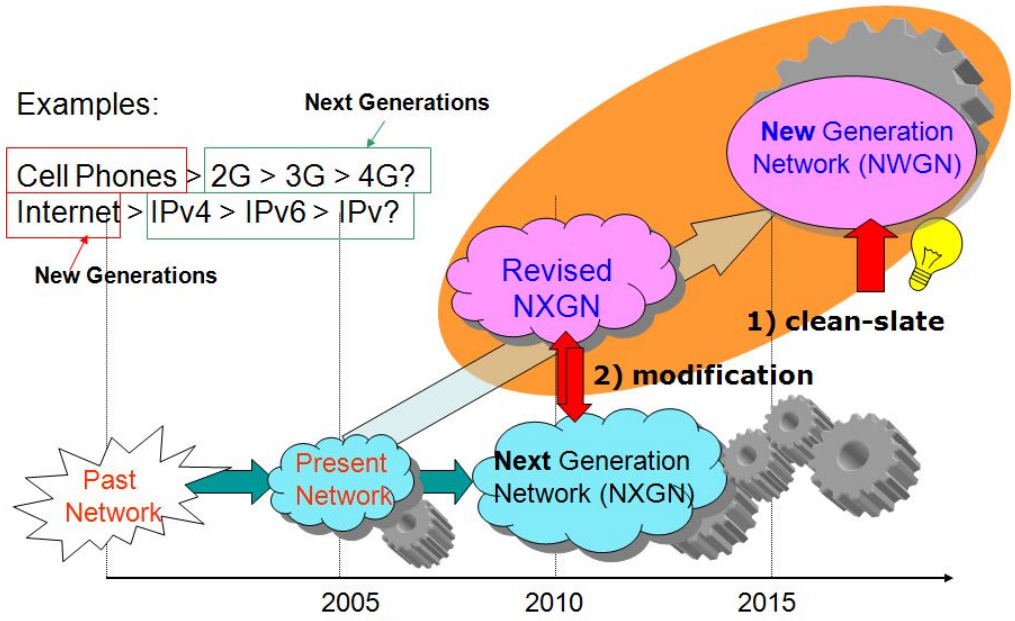
② 다양한 분석 기법에 의한 데이터 보강.

③ 위협 분석

3. 일본

가. 개요

일본에서는 현재 인터넷에 기반한 차세대 네트워크에 대한 연구인 ITU-T 표준 기반의 NGN을 NXGN이라고 명칭을 변경하고, 일보에서 보는 미래 인터넷을 신세대 네트워크라고 구분하여 2007년부터 5년가 300억엔(4,500억원)을 투자하여 신세대 네트워크, 즉 NWGN에 대한 연구를 새롭게 시작하였다. 새로운 패러다임 기반의 NWGN 완성은 장기적인 과제이기 때문에 현재 인터넷의 점진적 개선인 NXGN에 대한 연구/개발과 NWGN에 대한 연구를 동시에 진행하고 있다.



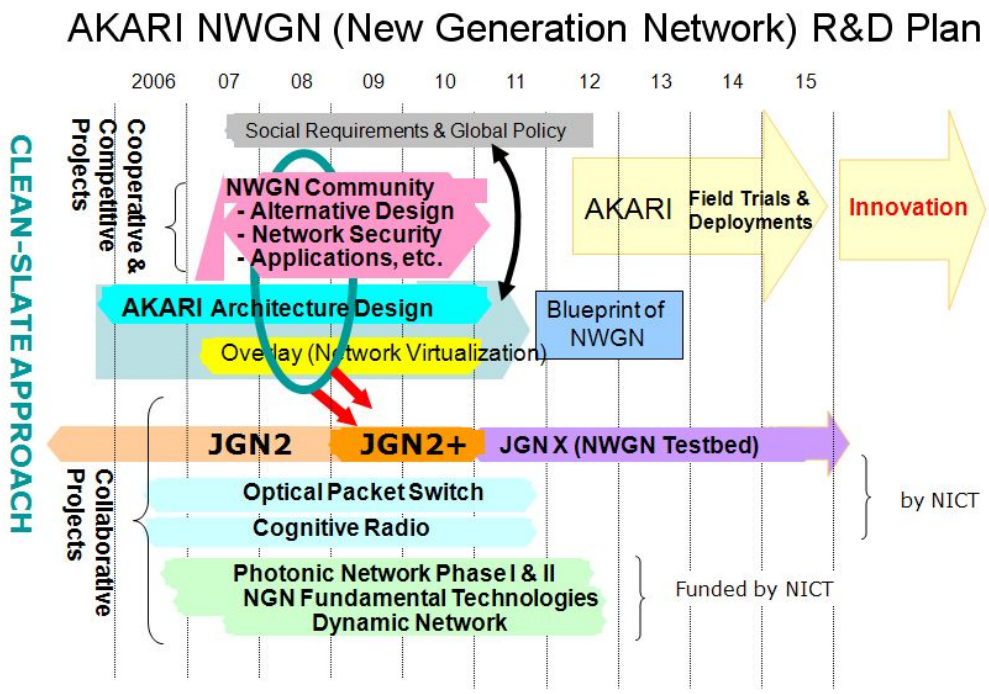
<그림 6> NXGN 과 NWGN의 관계

출처: Hideki Otsuki, "AKARI and JGN2plus", NICT, 2008. 3.

미래인터넷인 NWGN에 대한 연구는 국책연구소인 NICT의 Network Architecture Group이 주도하고 있으며, NWGN의 아키텍처를 설계하는 AKARI프로젝트를 2006년부터 시작하였다. 일본은 2011년까지 NWGN 아키텍처 설계를 완료하고 이를 구현시험하면서 2015년에 완성한다는 계획을 진행 중이다. 일본의

AKARI 프로젝트는 2008년에 NWGN의 기본 설계원칙과 일부컴포넌트의 구조에 대한 초안을 포함하는 NWGN 개념설계서 v1.1을 발표하였다. 이 개념설계서에는 NWGN의 구성요소로서 광 패킷스위칭과 광 패스 스위칭이 결합된 optical core 망, 새로운 광액세스망, 패킷기반 무선다중접속방법, ID/Locator 분리주소체계,

cross layer 구조, 보안구조, QoS 라우팅, 보다 단순해진 IP layer 구조, 네트워크 가상화등을 포함하고 있다. 그리고 일본은 미래인터넷를 위한 테스트-베드구성을 위해를 2002년과 2006년에 각각 e-JAPAN과 u-JAPAN 프로젝트 시작했고 인터넷 이키텍처 디자인인 NGN을 수행하고 있으며, 2004년부터는 JGN2를 시작했고, 2012년까지 Post-JGN2라는 이름으로 연구를 계속 진행할 예정이다.



<그림 7> NICT 추진 계획

출처: Hideki Otsuki, "AKARI and JGN2plus", NICT, 2008. 3.

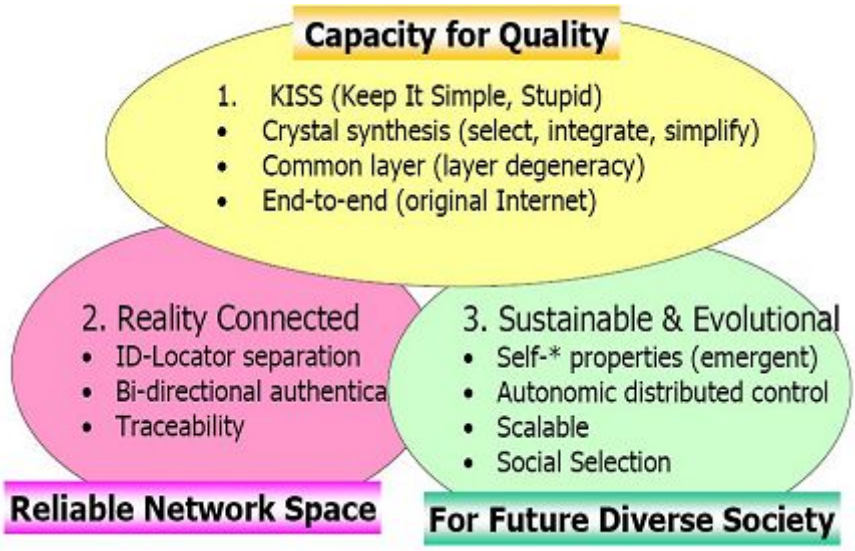
NICT에서 지원하는 과제들 중 AKARI 프로젝트는 전반적인 NWGN(New Generation Network)을 위한 아키텍처 설계를 목표로 한다. NWGN은 기존의

NXGN(Next Generation Network)와 구분되는 개념으로 기존 인터넷의 제약조건을 고려하지 않는(clean-slate) 완전히 새로운 미래 인터넷을 의미한다. AKARI 프로젝트는 현재 개념적인 로드맵 구축을 마치고, 테스트베드 설계와 기반 기술 연구에 집중하고 있는 단계이다.

나. 일본의 미래 인터넷 보안

1) AKARI 프로젝트

AKARI 프로젝트에서는 미래인터넷의 요구조건 중 하나로 보안을 강조하고 있다. 현재까지 미래인터넷의 보안 기술에 대한 구체적인 연구를 수행하고 있지 않지만, 다음과 같은 설계 원칙을 기반으로 보안이 강화된 네트워크 아키텍처 설계를 추진할 계획이다.



<그림 8> 보안성이 강화된 미래 인터넷 아키텍처

출처: Hideki Otsuki, "AKARI and JGN2plus", NICT, 2008. 3.

정보통신 네트워크는 개인과 조직의 모든 사회적 활동에 있어 필수 불가결한

존재이며 이의 기능 유지를 위해서는 네트워크 자체의 안정성과 신뢰성을 확보하는 것이 중요하다. 이를 위한 과제로 여기서는 고도의 내장애성 및 장애로부터의 신속한 복구, 인위적인 실수와 사이버 공격 상황에서도 안정적 운용이 가능한 서비스의 보장, 안전성과 신뢰성이 확보된 네트워크 이용환경, 전사회적 규모의 네트워크 트러스트 기반의 구축을 들고 있다.

실제로 사이버 공격뿐만 아니라 시스템의 대규모화에 따른 인위적 실수를 포함한 장애의 발생은 불가피하며 이러한 취약성을 전제로 한 지속가능하고 안정적인 네트워크의 실현이 중요하다. 또한 이용자의 입장에서는 네트워크화된 생활환경에서 제공되는 각종 서비스의 신뢰성 향상에 대한 요구가 높아지고 있다. 이에 대응한 신뢰할 만한 네트워크의 실현을 위해 다음의 두 가지 과제를 들 수 있다.

① 네트워크 자체의 안정성 및 신뢰성 확보

지속적이고 안정된 네트워크 기능의 제공을 위해 유저 단말기에서 네트워크 인프라와 온라인 서비스에 이르기까지 일관된 상호의존적 네트워크 기술이 요구되고 있다. 이를 위해서는 고도의 내장애성 및 장애로부터의 신속한 복구기능과 사이버 공격이나 인위적 실수와 같은 취약성을 전제로 하면서 안정적인 네트워크 운용을 실현하는 기능이 필요하다. 그리고 이러한 네트워크 자체의 서바이벌리티(생존가능성)와 함께 재해 등의 비상시에 일반인의 생존가능성을 높일 수 있는 사회규범의 정비가 또한 중요하다.

② 서비스와 네트워크 엔터티에 대한 신뢰성 확보

온라인 상의 공공 서비스나 은행업무와 같은 사회적 환경을 아우르는 네트워크에서는 개인과 기업 등 거래상대의 네트워크 엔터티에 대한 신뢰성을 확보할 수 있는 환경이 요구되고 있다. 이를 위해서는 향후에 도래할 유비쿼터스 환경을 감안한 고도의 보안기반기술과 개인인증기술, 개인정보보호기술, ID 관리기술, 서비스 신뢰성기술과 같은 트러스트 기반기술을 확립하는 것이 필요하다.

위와 같은 두 가지 과제를 위해 네트워크사회 기반 기술과 네트워크 기반 기술을 통해 아래와 같은 로드맵을 제시하고 있다.

2) 네트워크사회 기반기술과 로드맵

인터넷과 정보통신 네트워크는 이제 개인과 사회의 라이프라인이 되었으며 따라서 네트워크의 지속적이고 안정적인 가동은 대단히 중요한 문제가 되었다. 이를 위해서는 사이버공격에 대한 내장애성과 장애 발생 시에도 신속한 복구가 이루어질 수 있는 네트워크의 기능을 실현하는 것이 중요하다. 또한 시스템의 오작동과 인위적인 실수 등의 취약성을 전제로 한 시스템 전체의 치명적인 장애를 피할 수 있는 기능을 실현하는 것이 필요하다. 이러한 지속적이고 안정적인 네트워크의 내장애성을 단말기에서 인프라에 이르는 각 계층에 실현하는 것이 사람과 사회를 지원하는 통신네트워크의 근간이 될 것이다. 그리고 네트워크 상의 단말기에서 인프라 서비스에 이르는 각 계층에 신뢰성을 위해 다음과 같은 기능들이 요구 된다.

<표 4> 네트워크 각계층의 신뢰성을 위한 기능

구분	필요 기능
네트워크상의 단말기	버퍼 오버 플로우(buffer over-flow) 공격 탐지 및 회피기능
	불법프로그램 탐지 및 제거기능
	과도한 네트워크 폭주 제어기능
	파일 및 메모리영역의 액세스 제어기능
보안성 갖춘 운영체제	자율적인 경로제어와 네트워크 재구성 및 폭주 제어기능
	고도의 리던던시(Redundancy) 관리기능
	자동적인 불법 트래픽 탐지 및 배제기능
	고정노드에 대한 부하분산기능
	가상네트워크 관리기능
서비스 API	부정한 서비스이용의 탐지 및 회피기능이 필요하다.

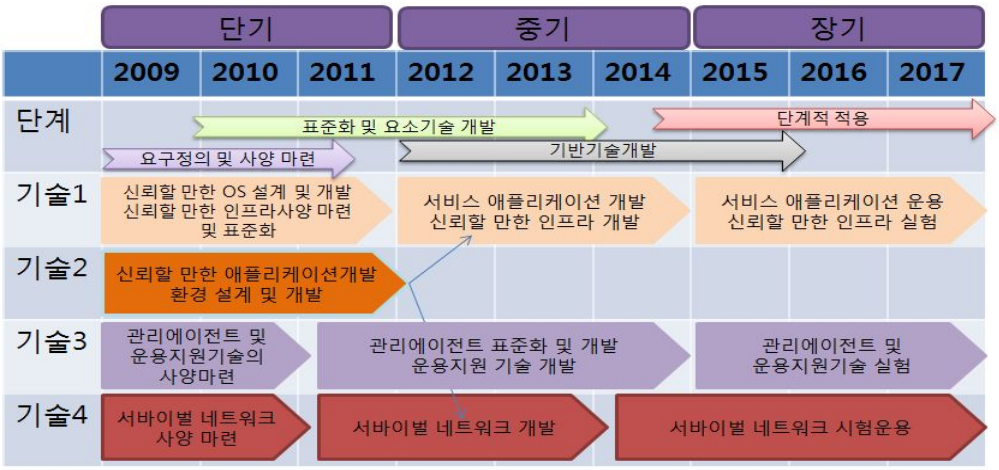
출처: 일본 정보통신연구기구, 신세대 네트워크 기술전략, 2009. 3..

그리고 개개의 서비스 애플리케이션 개발자가 취약성이 내포된 프로그램을 작성함으로써 많은 보안사고가 발생하고 있으며, 네트워크운용에서도 네트워크 관리자의 부담이 커 다양한 인위적 실수가 일어나고 있다. 이를 피하기 위해서는 프로

그래밍의 위협 요소를 지원하는 기술 및 탐지, 검증기능을 가지면서 보안성을 지닌 컴파일러의 개발과 네트워크 트래픽 중계장치가 고도의 자율성을 지니는 것과 함께 관리자의 운용작업을 최소한으로 제어할 수 있는 지원 기술이 필요하다.

기존의 네트워크에서는 인위적 실수로 인한 네트워크 정지가 빈번히 발생하고 있다. 구체적으로 보면 인터넷 서비스 제공업체의 관리자가 경로를 잘못 설정하여 인터넷 전체가 수 시간에 걸쳐 기능이 정지된 사례가 있다. 또한 대표적 보트넷인 멀웨어(악성코드)의 만연과 그에 따른 DDoS공격, 무차별적인 스팸메일 등의 현상은 오늘날 조직화된 범죄자집단에 의해 일어나고 있으며 심각한 사회문제가 되고 있다.

이러한 현실을 바탕으로 신세대 네트워크에서는 유저 단말기에서 네트워크 인프라에 이르는 포괄적인 대책을 마련하고 인위적 실수 및 조직적 범죄에 의해 초래되는 악영향에 대한 내성을 갖추어야 한다.



<그림 9> 네트워크사회 기반기술과 로드맵

출처: 일본 정보통신연구기구, 신세대 네트워크 기술전략, 2009. 3..

다. 네트워크기술과 로드맵[3)]

네트워크 사용자에게 있어 안전성의 확보와 이용환경에 대한 신뢰의 확보는

3) 일본 정보통신연구기구, 신세대 네트워크 기술전략, 2009. 3..

기본적인 문제이며, 네트워크화된 생활환경과 사회환경에 있어서의 안정성과 신뢰의 확보도 또 다른 중요한 문제이다. 따라서 이들을 지원하는 사회기반의 개발이 중요하다. 구체적으로는 네트워크 엔터티(서버 등의 통신기기) 차원뿐만 아니라 통신의 주체(개인과 조직) 차원에서 통신상대를 인증하고 '자신이 현재, 누구와 거래를 하고 있는가' 하는 것을 확실히 증명할 수 있어야 한다. 또한 사이버 범죄를 예방하기 위해 통신의 주체를 객관적으로 평가하는 제3의 기관을 설정함으로써 네트워크 사용자가 안심하고 서비스를 이용할 수 있는 시스템을 마련할 필요가 있다.

네트워크 사용자에게 있어 사이버 범죄와 개인정보 누설 등의 위험이 없는 보안성 있는 네트워크 환경과 신뢰성 있는 온라인 서비스는 매우 중요하다. 또, 보안상의 위협을 네트워크 사용자가 의식하지 않도록 하는 편리성도 필요하다. 유비쿼터스 사회가 도래함에 따라 네트워크화된 생활환경에서 단말기의 사용은 더욱 늘어나고 보다 다양화 되고 있으며 이에 대한 안전성과 신뢰성을 확보하는 것이 대단히 중요하다. 그리하여 이러한 안전성과 신뢰성을 바탕으로 개인정보 및 기밀정보의 누설을 최소화할 수 있다. 결과적으로 네트워크 사용자의 정보통신 네트워크에 대한 심리적 불안요소를 제거함으로써 네트워크의 활용을 보다 촉진하기 위해 다음과 같은 인증기술이 필요하다.

<표 5> 인증 기술

구분	필요 기능
네트워크인증 기반 기술	P2P형 통신에 맞는 인증기반기술
	운영체계(하위 레이어)와 결합된 인증기술
	간단한 인증설정기능
통신주체의 인증기반기술	ID 관리기술
	제3자에 의한 통신주체의 평가기반
고도정보관리 기술	정보의 통합 관리기술
	사생활 정보 및 기밀정보 보호기술
	데이터 변조방지기술

출처: 일본 정보통신연구기구, 신세대 네트워크 기술전략, 2009. 3..

4. 주요 국외 동향 분석

이상에서 살펴본 바와 같이 현재 미국, 유럽, 일본은 미래 인터넷에 관련한 다양한 프로젝트를 진행 중이며 프로젝트는 미래사회에서 큰 영향력을 차지하게 될 인터넷의 새로운 기반 구축과 그 기반에서의 새로운 서비스에 중점을 두고 추진 중에 있다. 각국에서는 현재 운용되고 있는 네트워크 기반이 많은 문제가 있음을 인지하고 미래의 새로운 서비스를 위해 현재와는 다른 새로운 개념의 네트워크 기반 구축을 추진 중에 있다. 자국 및 국외 산업체와 학계 그리고 국가간 협력을 통해서 미래 인터넷 구축에 있어 우위를 점하기 위해 박차를 가하고 있다.

그러나 아직까지도 각국에서 진행 중인 새로운 네트워크 개념은 확립되어 있지 않고 계속 실험과 테스트를 통해 정립중이다. 미국의 경우 세부적인 목표를 정하여 특정 기관에 일임 하지 않고 미래 인터넷이란 주제 아래 다양한 연구와 실험을 통해 최상의 결과를 나타내는 연구를 정하는 (bottom-up)형식으로 진행하고 있다. 유럽의 경우는 크게 미래 인터넷 2020 같은 모델을 선정하고 그 모델에 맞춰 실현 할 수 있는 방법을 위해 연구를 진행 중에 있다. 일본은 단계별 목표를 정하여 연구 및 실험을 진행 하고 있다. 각국의 연구 진행 방법의 차이는 조금씩 있으나 결과적으로는 비슷한 양상을 나타내고 있으며, 한 국가만으로 미래 인터넷이 확립되지 않는 것을 인지하고 상호간 교류중이다.

따라서 미래인터넷의 보안의 경우도 현재 미래 인터넷의 개념이나 체계가 확립된 상황이 아니므로 각국은 자국내에서 진행 중인 미래 인터넷 기반 프로젝트나 연구에 맞춰 보안 관련 체계를 구축하고 있다. 그리고 현재상황에서 보안의 문제가 되고 있는 위협이나 침해 사고 및 이슈가 되고 있는 개인정보 부분에도 관심을 보이고 있는 추세이다.

현재 진행 하고 있는 각국의 보안 정책들은 국가 차원의 보안 정책으로 서비스에 대한 보안 정책보다는 네트워크 기반의 신뢰성과 인증 및 프로토콜 개발에 중점을 두고 있다. 이러한 경우 첫 번째, 서비스는 네트워크 망에 종속되지 않는다고 볼 수도 있으며, 두 번째로 어떠한 서비스가 제공될지 알 수 없기 때문일 수도 있다.

미국의 경우 자국의 인프라와 미래 인터넷 관련 프로젝트 개발 상황에 맞는

보안 정책들을 수립하면서 같이 발전 시켜나가는 방식이며, 유럽의 경우 2020의 시나리오와 현재 인터넷에서의 이슈와 문제점을 비교하여 미래 인터넷의 위협을 예측하는 방법으로 구체적인 상황을 예상하며 추진중이며, 일본의 경우 역시 비슷한 형태를 띄고 있다. 이는 미국이 미래 인터넷 분야에서 우의를 점유 하고 있다고 볼 수 있으며, 아직은 많은 정보들이 오픈 되고 있지는 못한 상황이다.

기존의 인터넷은 보안이 적용되어 설계된 것이 아니라 확장이 되고 나서야 보안이 적용되었기 때문에 많은 문제점을 안고 있다. 각국은 이점을 인식하고 미래 인터넷 기반 구축 및 프로토콜 확립시 보안을 같이 적용하여 기반이 안전한 미래 인터넷을 구축하려 한다.

우리 정부가 미래 인터넷의 우위를 점하기 위해서는 기반 구축이나 기반 기술에 중점을 두고 기술 개발에 보안 적인 측면을 고려하여야 할 것이며, 미래 인터넷 개발 국가들과의 공조와 협력이 필요하다.

<표 1> 국외 미래 인터넷 추진 현황

구분	미국	EU	일본
관련 프로젝트	GENI	NFP	NWGN
주관 기관	미국과학재단(NSF) 산하 GPO 신설	FP7산하 FIRE 조직 신설	총무성 산하 NICT
정부 참여	정부 주도 약함 (미국과학재단 주관)	정부 주도 강함 (전담조직 FIRE 신설)	정부 주도 중간 (총무성 산하기관)
예산 및 기간	2005 ~ 2013 연간 약 1,500만불	2007 ~ 2013 총 7.67억 유로	2007 ~ 2015 72억엔('08) (300억엔/5년)
비전	인터넷 구조 개선으로 미래의 세계 인프라로 확대	미래 인터넷 구현으로 유럽의 산업 경쟁력 강화	언제 어디서나 통신에 고속으로 안정적인 접속이 가능한 유비쿼터스 서비스 제공
연구주제	미래인터넷 설계 및 테스트 인프라 구축	선도적 테스트인프라 구축 및 서비스 발굴	미래 유비쿼터스 통신망 기반 구축 - 광 기술에 편중, 네트워크 중심 연구
연구중심	테스트베드 구축 중심 (실험 위주, 실용적 접근)	기술/경제/사회 통합 연구 (미래인터넷 생태계 종합 논의)	네트워크 중심 연구 (광통신망 구축 편중)
시험망	PlantLab,GENI	PII, OneLab2	Core, JGN2plus (향후 JGNX)
보안 관련 현황	기존의 취약 인프라의 혁신적인 개혁	미래 사회 실현을 위한 전방위적인 연구	새로운 인프라구축시 기존의 취약점 보완
추진전략	모든 전문가 제안·경쟁 → 실험 검증후 결과 채택 (상용화를 통한 사업성 강조)	선정 프로젝트에 전문가 참여 → 결과 도출을 위해 협력 (유럽 독자모델 개발 중심)	광통신망에 자국의 경쟁력 특화 전략 (모바일, 가전, 게임 결합)

*GENI: Global Environment for Network Innovation, *NFP: Network of the Future Project *NWGN: NeW Generation Network. *NSF: National Science Foundation, *GOP: GENI Project Office, *FP7: 7th Framework Programme *FIRE: Future Internet Research and Experimentation *NICT: National Institute of Information and Communications Technology

출처: 방송통신위원회 자료 재구성.

제2절 국내 미래인터넷 환경구축 및 연구 동향

국내는 2006년에 들어서 '미래인터넷포럼'을 구성하여 학계 중심으로 연구를 시작하는 단계이다. 현재 미래인터넷과 관련하여 진행 중인 연구는 핵심기술 개발, 인프라플랫폼 및 네트워크모델 개발, 연구시험 환경 구축 등이 있다.

<표 2> 국내 미래인터넷 관련 연구개발 현황

연구명	연구내용	주관기관(예산)
①미래인터넷 핵심기술 연구(미래인터넷포럼 지원사업*)	전송기술, 보안, 이종망 연동, 미래인터넷 아키텍처 구성 등의 원천기술 개발	서울대학교 ('07~'09)
②미래인터넷 인프라 플랫폼 및 핵심원천기술 개발	네트워크 가상화 지원 프로그래머블 플랫폼과 핵심 원천기술 개발	ETRI('09~'13)
③미래인터넷 네트워크 모델 개발 (과학기술재단 지원)	콘텐츠 중심 네트워킹 모델링, 미래 무선네트워크 모델링과 알고리즘 연구	국가수리과학연구소('08~'14)
④KOREN 기반 Planetlab 연구시험 환경 구축	KOREN을 국내 테스트베드로 운영하기 위한 환경 구축	NIA, KAIST, KT

출처: 방송통신위원회

2006년 9월 발족된 미래인터넷 포럼은 아키텍처, 무선기술, 서비스 테스트베드, 정책 등의 5개의 워킹그룹을 구성하고 미래인터넷에 대한 논의를 시작하였다. 2007년에 정보통신부의 신성장동력 사업으로 "미래 인터넷 핵심기술 연구"(원천기술 연구분야) 선정되어 서울대학교를 주관기관으로 총 8개의 기관[4] 중심으로 3년간 총 36억의 정부출연금으로 정부핵심기술 선행 연구를 진행 중이다.

4) 서울대, 충남대, KAIST, ICU, GIST, 포항공대, 고려대학교, 첨단망협회(ANF)

< 연구 내용>

- 미래인터넷포럼을 중심으로 연구개발과제 발굴 및 상용화로 연계될 수 있는 연구기획
- 코어망 전송, 보안, 이종망 연동 등 미래 인터넷 아키텍처 구성 등의 원천 기술 개발 연구
- IETF, ITU 등의 미래 인터넷 표준화 동향 및 기술분석 보고서 작성
- GENI, EU-ICT FP7, AsiaFI 등 국제적 협력체제 구축진행중이다.

2009년부터 ETRI가 "미래 인터넷 인프라를 위한 가상화 지원 프로그래머블 플래폼 기술"이란 제목 하에 2013년 까지 정부출연금을 지원받아 미래 인터넷 테스트베드용 가상화 플래폼 개발을 시작하였다.[5)]

< 연구 내용>

- 미래인터넷 인프라 구축에 공통적으로 소요될 프로그램화 및 네트워크가상화 핵심 원천 기술 개발
- 다양한 미래의 신산업 지향 아키텍처 및 서비스 실현을 위한 네트워크 플랫폼 기술의 단계적인 개발

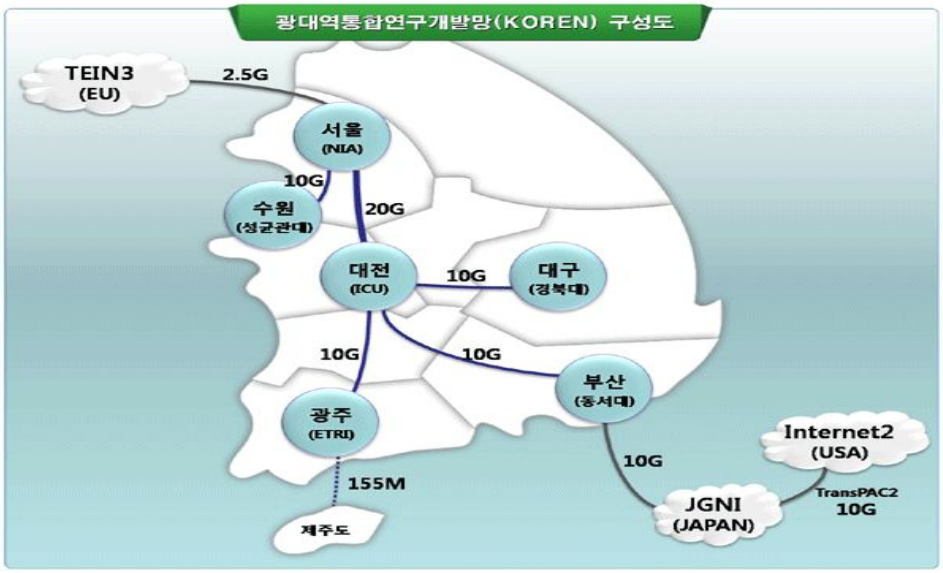
그리고 미래 인터넷 네트워크 모델 개발[6)]을 위해 국가수리과학 연구소, 서울대, KAIST에서 2008년부터 총 6년간 연구 진행 중이다.

< 연구 내용>

- 콘텐츠 중심 네트워킹 모델링, 미래 무선 네트워크 모델링, Massive data set에서 검색 모델 및 알고리즘 등 연구
- 현재까지 알려진 복잡계(사회연결망, 바이오 네트워크) 연구
- 그래프 모델 연구 등 기반수학 개발

---

5) '방송통신망 중장기발전계획'('09.1) 세부 정책과제(미래 네트워크 R&D 지원)로 반영
6) 기초기술연구회 지원과제



<그림 10> 광대역 통합연구 개발망 구성도

출처: .http://www.koren.kr/

미래 인터넷의 환경 운영 시험 및 테스트베드 구축을 위해 KOREN 기반 Planetlab 연구시험 환경: PPK(Private PlanetLab Korea) 구축 중이며 KOREN NOC[7]에서 직접 PlanetLab을 운영함으로써 KOREN 이용자가 보다 쉽게 PlanetLab을 사용할 수 있는 환경 제공하고 KOREN 기반의 한국 내 PlanetLab 테스트베드로서 국내 이용자들을 위한 PlanetLab 노드 관리 및 사용자 등록 등 NOC(Network Operating Center) 기능 수행을 위해 NIA, KAIST, KT가 참여 하고 있다.

7) 1995년에 시작된 비영리 연구망, 현재 서울, 대전, 광주 등 5개 사이트, 10개 노드 연결

제3장 인터넷의 미래상과 사이버 위협

제1절 인터넷의 미래상

1. 인터넷의 진전

지금의 인터넷은 1980년대 초 단순한 학술적 네트워크에서 시작하여 정보, 통신, 거래에 필요한 실질적인 세계적 공개 인프라로 성장하여 21세기의 성장동력으로 자리를 잡게 되었다.

인터넷의 트래픽은 매년 50~60%씩 장기간에 걸쳐 꾸준히 증가하여, 모바일 데이터량은 월 33PB[8]로 매년 100%이상의 급격한 증가율을 보이고 있으며, 디지털 융합에 따른 IT, 통신, 가전, 미디어 등 현대 산업의 지각 변동을 일으키는 원동력이 되고 있다.

신기술로 인해 경제적 가능성이 더욱 커지는 '롱 테일 현상(long-tail phenomenon)'과 사용자제작콘텐츠(User Created Contents)가 선풍적인 인기를 끌고 있고, 소셜네트워킹서비스와 같은 새로운 애플리케이션의 출현으로 의사소통 방식이 변화되고 있다. 또한 이전에는 온라인 접속의 유일한 방법이 PC를 이용하는 것이었으나, 휴대전화, PDA, 게임기, TV 등의 다양한 단말장치로 변화가 이루어지고 있다.

향후의 미래인터넷은 기존 인터넷의 진화가 아닌, 전혀 새로운 인터넷을 구상하고 있다. 새로운 아키텍쳐와 인터페이스, 데이터 관리, 그리고 모든 사물, 센서, 서비스, 사람을 통합하는 새로운 방식의 미래인터넷이 출현할 전망이며, 2020년이 되면 인터넷은 공공 인프라로 자리 잡고 서로를 연결하는 물리적 대상들에 의해 역동적으로 창조될 것이다. 이러한 미래인터넷은 새로운 서비스를 풍부하게 제공할 것이며 오늘날의 인터넷보다 사회경제적으로 훨씬 더 큰 영향을 미치게 될 전망이다.

---

8) 1PB(페타바이트)=1015엑사바이트(또는 100만조 바이트)

2. 미래인터넷 사회의 전망(~2020년)[9]

가. 개인의 글로벌 네트워크

< 네트워크 2020: 움직이는 정보 >

매티는 전기 자동차를 타고 사무실로 향한다...사무실에 도착한 매티는 자동차를 회사의 충전 포인트에 연결한다. 그의 자동차는 전력회사와 협상을 할 수 있을 만큼 충분한 지능을 갖고 있어서 가장 저렴한 요금으로 전력을 공급받을 수 있다. 사무실의 시스템은 매티의 바이오인식정보를 통해 그를 자동으로 인식하고 관련 문서를 불러온다. 이와 동시에 전화기가 무소음 작업 모드로 전환된다. 원격회의를 하는 동안에 매티가 모든 참석자들에게 프리젠테이션을 하면, 모든 회의 현장의 대형 디스플레이에 그대로 나타난다...회의가 끝나고 매티의 전화가 울린다. 매티의 상사는 매티의 상태가 '휴식 모드'로 전환되었다는 통보를 받았고, 그 기회를 이용해서 실험실의 시험결과에 대해 어디에서 논의할 것인지 그에게 전화를 건 것이다…퇴근후 거실에서 매티는 이탈리아 세리아A의 실시간 축구경기를 시청한다. 그는 3D 웹캐스트를 즐긴다. 패널티킥을 하는 동안 그는 패널티킥이 어디로 날아갈지 예상하면서 골포스트 사이에서 카메라 각도를 조정한다.

모든 시스템 간 끊김 없는(Seamless) 통신이 지속되어 시스템과 기기들이 인간의 현재 상황에 맞는 행동을 시간지연 없이 즉각 수행할 수 있게 된다. 모든 환경(집, 사무실, 자동차 등)이 상황을 인식하고 인식한 상황에 대한 정보를 공유함으로써 언제 어디서나 유비쿼터스형 서비스를 제공하게 되며, 자신의 개인정보를 어디에서나 언제나 이용할 수 있으며 이를 바탕으로 개개인에게 특화된 콘텐츠를 제공하게 된다. 또한 기반시설을 재구축하거나 장비를 교체하는 일 없이 가상화 서비스를 통해 유지·보수비용을 절감할 수 잇게 된다.

이렇게 시스템 구성요소들 간의 기술발전 속도 차이는 전체 시스템의 발전 속

9) KISA, EU의 미래인터넷 전망 및 전략, CSO브리핑(2009. 7)
EU, 미래인터넷 2020(Future Internet 2020), 2009: 미래인터넷 분야의 공공-민간 협력 방안 마련을 위해 유럽 위원회가 유럽의 고위급 전문가들을 초청하여 발간한 보고서로 다양한 전문가들의 경험, 지식, 정보들을 토대로 기술 및 서비스 관련 다양한 접근을 시도하여 미래생활상을 구체적으로 묘사한 시나리오를 구성, 실제 미래상을 그려봄으로써 미래인터넷의 성공적 실현을 위해 준비해야 할 부분들을 보다 다차원적으로 탐구하고 포괄적으로 분석·검토하고 있다.

도를 늦추는 저해요소로 작용할 수 있다. 그리고 대용량 무선 통신에 사용되는 주파수 이용을 최적화 하고 시장원칙의 마련이 필요하다. 이는 주파수는 유한 자원이므로 무선 접속성과 이동성, 대용량 데이터 교환을 효율적으로 수행하는 새로운 주파수 활용 패러다임이 필요하게 되는 것이다. 대규모 데이터 센터의 전력소비 급증이 에너지와 환경에 미치는 영향을 고려하여 전력공급을 최적화하고 전력소비를 줄이는 노력도 필요하게 되며, 무선 네트워크의 사용료를 낮추고 상호운용성을 보증하기 위해서는 국제적 합의를 통한 무선 네트워크 공개표준 수립이 필요하며, 영향력 확보를 위한 디지털 자원통제 시도 등, 이해관계자들의 입장 차이가 시장장벽으로 작용하여, 비능률적인 시장구조가 형성될 수 있다. 또한 국가나 지역간 서로 다른 법률 및 규제가 정보와 콘텐츠의 자유로운 이동을 방해하여 시장 활성화의 장벽으로 작용할 수도 있다.

나. 웹기반 서비스 경제

< 피에르 체육관에 가다 >

일요일 아침, 피에르는 체육관에 가려고 일찍 일어났다. 식탁에 앉으면서 플렉서블 디스플레이를 펼치고 피에르가 관심을 갖는 내용 중심으로 편집되어 있는 맞춤식 일요신문을 읽는다. 신문에는 토요일부터 시작된 포뮬러1 레이싱 예선 결과에 관한 동영상이 연결되어 있다. 자동차 경주 열혈 팬인 피에르는 오늘 저녁 경기를 최적의 조건에서 즐기기 위해 쌍방향 3D 고화질 전송서비스를 예약한다…피에르는 체육관에서 운동을 시작한다. 최신 전신운동 기구에서 운동을 하면서 장착된 화면을 통해 비즈니스 관련 이메일을 확인한다. 소형 보안 RFID 기반 전자키를 통한 로그인으로 통신의 보안을 유지한다. 이 전자키는 집과 자동차, 사무실 출입에 필요한 만능키로 이용하며, 체육관에서는 피에르의 운동계획을 저장하고 진도를 모니터링 한다…피에르의 아들 앙리는 숙제를 하기위해 학급 전체가 공유하는 학습 공간에 들어가서 역사 과제를 설명하는 선생님의 영상 메시지를 본다…앙리는 숙제를 한 다음 이를 수업 전에 선생님이 살펴볼 수 있도록 선생님의 서류함에 제출한다.

인터넷을 활용한 차세대 서비스는 디지털 세계와 물리적 세계를 통합하는 '사물의 인터넷(Internet of Things)'에 긴밀하게 의존하게 될 것이다. 언제나 광대역

인터넷 접속이 가능한 쌍방향 방송 미디어가 출연하게 되고, 디스플레이 기술이 더욱 발전하여 주변 환경이나 특정 장치에 쉽게 통합되는 초박형, 플렉서블, 고화질 3D 디스플레이 장치의 양산이 가능할 것이다.

풍부한 영상 서비스를 제공하는 초광대역 네트워크로, 2020년까지 가정용 광대역 네트워크는 초당 10GB, 모바일 1GB의 속도로 풍부한 영상을 제공하는 인터넷 서비스 제공이 가능할 것이다. 유선 인터넷이 TV와 영상 전송 서비스의 주된 공급방식이 될 것이며, 모든 영상 기반 서비스를 동일한 네트워크를 통해 동일한 장치에 공급할 수 있게 되어 서비스 융합이 가속화될 것이다.

서비스의 융합으로 전략적, 기술적, 상업적 시너지 효과가 발휘되며, 특히 미디어와 오락, 방송, 출판에 큰 영향을 미칠 것이다. 디지털 영화 시장의 축소로 박스오피스의 경제적 중요성은 축소되고, 극장은 스튜디오의 마케팅 도구 등으로 남게 될 것이며, 주문형 영화, 비디오, TV시리즈의 콘텐츠, 사용자가 제작하는 콘텐츠 등 다양한 영상물에 기반한 오락물과 TV의 경쟁이 예상된다. 또한 게임을 통해 공동생활 경험을 할 수 있고 친구와 가족을 게임에 초대하는 등 게임, 소셜 네트워크, 비즈니스의 경계가 허물어지게 될 것이다.

< 내 차 어때요? 내가 직접 설계했어요 >

헬가는 오늘 새 차를 사러 간다. 새로운 차의 엔진은 전적으로 컴퓨터에 의해 작동되므로, 최대 성능 한계 내에서 필요에 따라 맞출 수 있다. 그녀는 주로 시내에서 운전을 하기 때문에 성능은 떨어지더라도 판매가격이 낮은 차를 선택했다. 나중에 언제라도 마음이 바뀌면 성능을 올리기 위해 무선으로 업그레이드가 가능하다. 물론 성능을 향상시키기 위해 프로그램을 다운로드 하려면 비용을 지불해야 하며, 단기간 업그레이드 요청도 가능하다…딜러는 헬가가 실시간으로 자신의 운전습관을 공개하면 자동차 보험료를 할인 받을 수 있다고 설명한다. 초보운전자인 헬가의 아들이 운전을 할 때 성능을 자동으로 낮추는 옵션을 선택하면 보험료를 절약할 수 있다. 헬가는 한동안 자신이 선택한 사양이 업로드 되기를 기다린 후 반짝반짝 빛나는 새 차를 타고 집으로 돌아온다.

모든 제품이 서비스 형태로 제공되고 변환 가능한 웹 기반 서비스 경제로 변환될 것이다. 사용자가 자동차에 새로운 기능을 요구할 수 있고, 기존의 성능을 바

꿀 수 있다는 사실은 자동차가 하나의 서비스로 변화된 사례라고 볼 수 있다.

사용자의 요구와 취향에 맞는 '맞춤형 시장'이 탄생하게 되어 사용자의 신상정보와 결합된 새로운 정보를 바탕으로 사용자의 요구와 취향에 맞는 독특한 제품을 공급하게 될 것이다. 기업은 맞춤화 과정을 단순화하고, 인간과 기계 사이에서 가장 쉽고 매력적인 인터페이스를 제공하게 된다.

제품의 서비스화에 따른 기업과 고객의 관계도 변화하게 된다. 제품을 서비스로 인식함에 따라, 중간 상인을 생략하고 생산자·제조자와 보다 직접적인 관계를 형성하게 되며, 유통과 같은 전통적인 중개 기능은 쇠퇴하는 반면, 끊임없이 고객 경험이 창조되고 서비스를 통합하는 시장 주체들이 새롭게 등장하게 된다.

이렇게 가상시장, ICT 지원 서비스, ICT로 통제되는 공급망이 증가함에 따라 인프라 보안 등 전체시스템의 신뢰와 보안이 중요한 해결 과제로 부각될 것이다.

그리고 신 서비스 경제에서 개인정보의 빈번한 확인 및 교환, 상황에 따른 정보 공개 수준 변화 등으로 ID 관리, 보관, 인증이 중요한 서비스로 발전하게 될 것이다.

서비스 경제의 맥락에서 유선 네트워크와 무선 네트워크 사이에 적절한 균형을 확립하는 것이 중요하게 되며, 상호운용성 보장과 규모의 경제 실현을 위해 미래인터넷 표준화 체계가 필요하게 된다. 특히 표준화는 사업에 필요한 지식 서비스를 제공하며, 자동화된 비즈니스 프로세스로 전환하기 위해서도 필요하다.

다. 사물과 연결된 인터넷 (An Internet with Things)

< 스미스 가족 스키타러 가다 >

스미스 가족은 휴일에 스키를 타러 간다. 탑승 후, 차량에 장착된 정보시스템이 그들을 환영하고, 가족은 그 정보시스템과 상호작용하며 여행계획을 세운다. 차량의 시스템이 길을 따라가면서 흥미로운 명소들에 대한 정보를 수집하여 도중에 만나는 장소들에 대해 설명을 하며 여행에 재미를 더해 준다. 불행히도 피터는 방금 지나친 고성의 사진을 찍을 기회를 놓쳤다. 하지만 그는 차량 통신장치를 이용하여 후행 차량 중 하나에게 사진을 찍어서 전송해줄 것을 부탁한다…가족은 무사히 겨울 스포츠 휴양지에 도착한다. 저녁 식사전에 피터는 샤워를 하기로 한다. 그가 욕실에 있는 동안 그는 거울을 통해 이메일을 확인하고, 경제나 정치 뉴스와 같은 피터가 관심 있는 정보와 함께 집에 있는 어머니에게 아무런 문제가 없다는 것을 확인한다. 저녁식사 후 가족은 객실로 돌아와 내일 스키 탈 준비를 한다. 호텔의 오락 시스템은 가족의 운동 이력과 슬로프 상태에 대한 예측자료를 바탕으로 다음날에 대한 제안을 해 준다…긴 하루를 보내고 피터와 칼라는 그 날 그들이 스키를 타고 내려온 활강코스를 서로에게 보여준다. 오락 시스템이 스키에 달린 초소형 센서로 수집한 위치, 가속, 속도와 같은 데이터를 바탕으로 그들의 개별적 경로를 재구성하여 경험과 흥분을 공유하게 해 준다.

사물의 인터넷(Internet of things)은 센서에 의한 상황인지 데이터, 사물간의 통신으로 수집한 데이터 등을 분석하여 인간에게 최적의 서비스를 제공하는 네트워크를 말한다. 그리고 사물과 연결된 인터넷(Internet with things)이라는 것은 사물의 인터넷(Internet of things)과 인간의 인터넷 정보사회가 결합되는 형태를 지칭한다. 즉 인간・사물・시스템 등 모든 것이 연결되어 미래인터넷 사회의 궁극적 모습을 달성한다는 것이다. 기존의 사물의 개념이 변화하여 사물은 단순한 물리적 대상이 아니라 물리적 실체와 디지털 정보의 끊김없는(seamless) 혼합물이라 할 수 있다. 그리고

미래사회에서는 센서네트워크와 인터넷의 발달로 인해 물리적 공간과 디지털 공간이 점차 일치되는 현상이 나타나게 될 것이다. 센서네트워크를 통해 수집된 주변 환경 정보와 인터넷상의 정보를 활용하여 이용자에게 유용한 서비스를 즉각적으로 제공하게 된다. 사물의 디지털 정보, 인간의 인터넷 정보가 결합되어 실생

활과 디지털 세상의 경계가 점차 모호해질 것이다.

거의 모든 사물에 센서와 메모리 장치가 장착되어 "사물의 인간화"로 칭할 수 있을 만큼 인간과 닮은 모습으로 존재하게 될 것이다. 다른 사물 및 인간과의 상호작용을 통해 축적된 정보를 활용하여 사물들이 점차 인간과 비슷한 방식으로 행동하게 되고, 클릭(point-and-click)으로 사물의 수행이 이루어지던 기존의 인터페이스는 사용자의 제스처나 언어 등의 새로운 매커니즘과 공존하게 된다.

정보를 활용하여 비즈니스 프로세스를 개선하고 새로운 프로세스 창조하게 된다. 위치, 물리적 특성, 상황 등의 이용 가능한 정보를 활용한 지능형 제품을 개발하여 비즈니스 프로세스 관리와 의사결정 과정에 활용하게 된다.

< 세탁기와 대화하다 >

마리오는 세탁을 할 준비를 하고 있다…많은 새로운 옷들이 '실크, 모직, 면, 레이온'보다 훨씬 좋은 자가세탁이 가능하고 나노 부품이 내장된 정교한 직물로 만들어져 있다…각 의류에 필요한 복잡한 세탁 요구사항을 다루기 위해, 옷이 세탁기에 말을 한다. 그리고 세탁기는 다시 의류 생산자와 세제 생산자에게 말을 한다. 세제 생산자는 마리오의 세탁기에 이 상황에 맞게 특수하게 개발된 특별 세탁 프로그램을 이용할 것을 권한다. 그 프로그램은 마리오에게 그에 대해 1유로를 지불할 의사가 있는지 묻는다. 안전한 세탁을 원하는 마리오는 지불을 동의한다. 그러면 세탁기가 세제 생산자에게서 세탁으로 인한 모든 문제로부터 마리오를 보호하는 보험증서와 함께 소프트웨어를 다운로드 받는다. 세탁기는 이런 식으로 에코시스템에게 말을 할 수 있다. 그것이 인터넷의 일부분이기 때문이다. 그리고 대화를 쉽고 재미있게 만드는 짤랑짤랑 소리를 내는 쌍방향 화면 덕분에 마리오에게 말을 할 수 있다.

다양한 시스템과의 통신을 통해 원하는 정보의 취득과 의사결정이 가능할 것이다. 통신비용의 절감이나 유비쿼터스형 접속성 실현을 통해 언제 어디서나 다양한 시스템과 통신이 가능하게 된다. 일상생활에서 수시로 발생하는 의사결정의 순간에 저비용의 신속한 정보취득은 인간이 효율적이고 명확한 판단을 내릴 수 있도로 지원한다.

모든 사물을 비즈니스 플랫폼으로 인식하게 된다. 이는 하나의 사물과 관련된

모든 생산자들의 정보가 융합되어 소비자에게 제공되는 새로운 비즈니스 패러다임이 될 것이다. 각 사물의 가치 사슬과 관련된 모든 당사자들에게 수익원으로 작용하고 신종 비즈니스 플랫폼을 통해 기업가치 상승 등의 이익을 창출하게 될 것이다.

< 개인별 맞춤식 매쉬업 >

안나는 쇼핑을 좋아한다…그녀가 진열대로 가까이 가면 오직 그녀만을 위해 특별 할인 품목을 알리기 위한 색상 코드와 함께 그녀의 사이즈에 맞는 옷들을 표시하는 작은 LED가 켜진다. 그녀가 탈의실로 가면 거울처럼 생긴 화면이 그녀를 인식하고 입어볼 옷들에 대한 선택을 가상으로 제시한다. 그녀의 사이즈를 알고 있는 가게의 컴퓨터는 화면에 나타난 그녀의 이미지에 옷을 입히는 작업을 쉽게 할 수 있다. 안나는 마음에 드는 옷을 발견하고 판매 사원에게 실제 옷을 가져다 달라고 부탁한다. 그녀가 옷을 입어보면 거울이 그녀의 이미지를 비추고 몇 가지 액세서리를 제안한다…안나의 친구들도 역시 합류할 수 있다. 새로운 소셜 네트워크 애플리케이션으로, 안나는 그 자리에 없는 친구 케이티에게 옷 입은 모습을 보고 조언을 요청한다. 그녀의 친구는 텔레비전이나 휴대전화 또는 네비게이션 화면 등의 장치를 통해 거울에 접근할 수 있다. 안나는 옵션에 대해 이야기한다. 그 옷에는 인터넷 주소가 있기 때문에 케이티 자신도 (가상으로) 옷을 입어볼 수 있다. 또한 가게의 재고품 중에서 다른 색상이나 다른 소재의 천을 선택할 수도 있고, 또는 그들이 함께 파티에 갈 때 그 옷이 얼마나 잘 어울릴지, 어떻게 보일지 살펴볼 수 있다.

다양한 콘텐츠나 서비스를 제공하는 매쉬업(Mashup)[10]은 미래인터넷의 핵심적 비즈니스 동인으로 작용할 것이다. 특정 상품에 관련된 정보와 콘텐츠의 조합을 통해 소비자에게 즉각적이고 다양한 서비스를 제공하는 비즈니스를 창출할 수 있다. 매쉬업 시장의 활성화를 위해서는 다량의 정보와 서비스가 소비자에게 무료로 제공될 필요가 있다.

소셜 네트워킹을 통한 소셜 리테일링(Social Retailing)의 시대가 다가올 것이다. 상품 구매 시, 네트워크를 통해 주변인들과 즉각적인 의견을 주고받는 등 소비자 개개인의 소셜 네트워킹이 상품 판매에 직접적인 영향력으로 작용하게 된다.

10) 매쉬업(Mashup) : 다수의 정보원으로부터 제공되는 정보나 콘텐츠를 조합하여 하나의 서비스로 제공하는 웹 사이트 또는 애플리케이션

물리적 위치에 관계없이 여러 기업과 개인들이 인터넷을 통한 시장 공간을 형성하며 기업이 고객에게 다가갈 수 있는 방식의 변화를 초래할 것이다.

새로운 애플리케이션과 서비스 사이의 상호운용성을 촉진하고 자유로운 경쟁을 보장하기 위한 플랫폼이 개방되고, 기업 및 사용자들이 다양한 서비스를 개발할 수 있도록 플랫폼을 개방하여 자유로운 경쟁을 보장하고 부가가치 창출을 극대화할 수 있다.

언제 어디서나 끊김 없는 유비쿼터스형 접속이 보장될 것으로, 대규모 정보를 활용하고 적절한 서비스를 실시간으로 제공하기 위해서는 언제 어디서나 데이터의 검색 및 접속이 보장되어야 한다.

새로운 인터넷 환경에 부합하는 규제 체계가 마련되어야 한다. 인프라의 공유를 바탕으로 창출된 새로운 서비스에 대해 참여자들 간의 신뢰를 구축하고 공정한 수익배분을 유도할 수 있는 규제 환성을 조성하고, 네트워크화 된 시스템에서 이용되는 데이터 소유권에 대한 기준이 마련되어야 할 것이다.

물리적 인식 시스템을 모든 사물에 적용할 수 있는 기술 및 경제성이 필요하다. 특정 사물에 따라 적절한 기술과 틀을 적용하고 서로 다른 종류의 기술이 적용된 사물들 간에도 자유로운 통신을 가능케 하는 기술적 융합이 필요하고, 모든 사물에서 ID확인이나 통신이 가능하기 위해서는 인식 장치 부착이 경제적으로 실현 가능한 정도의 저비용으로 가능해야 한다.

개인정보보호 및 서비스 안전성이 보장되어야 한다. 자동으로 수집되는 개인정보와 이를 활용한 서비스들의 안전성을 보장할 수 있는 새로운 네트워크 아키텍처와 프로토콜의 개발이 필요하다.

라. 새로운 규제 공간

< 나의 개인 블랙박스 >

바클라프는 일상생활이 디지털 공간에 쉽게 포착, 저장되고, 처리되어서 사소한 일을 모두 기억 할 필요가 없어졌다. 휴대폰의 저장용량이 테라바이트에 달해, 바클라프의 생활 속의 모든 데이터를 저장하고 남을 정도이다. 손에 휴대전화만 들고 다니면 대화 내용이 전화에 기록되고 저장되어 나중에 다시 들을 수 있으며, 문장에서 '의미'를 파악할 수 있다…바클라프는 상점에서 물건을 구매 할 때 결제 장치가 그의 휴대 전화나 다른 장치에서 돈을 인출한다. 동시에 거래 기록과 구매성격을 개인 메모리 공간에 저장한다. 바클라프가 구입하는 모든 것이 그의 개인 정보공간의 일부가 되어, 가상공간에서 사용하거나 실제세계로 행동이 이어질 수 있다…병원에서 바클라프의 건강상태 정보를 그의 블랙박스에서 다운로드하여 그의 라이프스타일과 숨겨진 병력 등을 이용하여 치료와 회복에 도움을 준다.

미래인터넷은 개인 삶의 일부로서 디지털 공간을 제공하며 제공된 공간에서 서로 정보를 공유하고 활용이 가능하고, 인터넷은 어디에나 내장되어 어디서나 접근이 가능하며 더 이상 인식되지 않는 동시에 다양한 당사자들이 제공하는 일련의 서비스로 변화될 것이다.

각각의 서비스나 상황에 따른 동적(Dynamic) 보안 기반의 ID관리를 통해 미래인터넷의 서비스는 내재적인 보안과 검증 보증을 요구하는 복잡한 웹서비스로 구성되고, 서비스들이 자동적으로 보안 수준을 선정해서 이용자의 편리성을 제공하게 될 것이다.

개인정보를 수집·분석 가공하여 디지털 블랙박스에 저장하는 서비스를 기반으로 새로운 비즈니스가 출현될 것으로 예상되며, 새로운 형태의 인터넷 사기나 개인정보 도용 등 윤리적 쟁점이 발생하게 될 것이다.

서비스 이용자와 제공자간의 근본적인 차이가 더 이상 존재하지 않는 서비스 경제에서는 모든 이해관계자와 인터넷 상의 주체들에게 책임을 부여하는 메커니즘이 필요하게 된다. 개인정보를 침해하지 않는 범위 내에서 사이버침해에 대한 효과적인 경고와 예방조치를 할 수 있는 관리 프로토콜이 필요하게 된다. 국경의 존재가 모호한 사이버공간에서 야기가능한 사이버 범죄, 세금 납부, 데이터와 지적

소유권 보호 등 경제·사회영역에 문제가 발생하게 될 것이다.

대규모의 데이터를 수집하고 분석하는데 있어서 중요한 저장 기술을 위한 물리적 장치와 클라우드 서비스 같은 기술이 필요하게 되고, 데이터 수집 장치의 끊김 없는 연결성을 보장하기 위해서 표준 및 규제정립과 통계적 접근법에 기초한 새로운 접근법이 필요하게 된다.

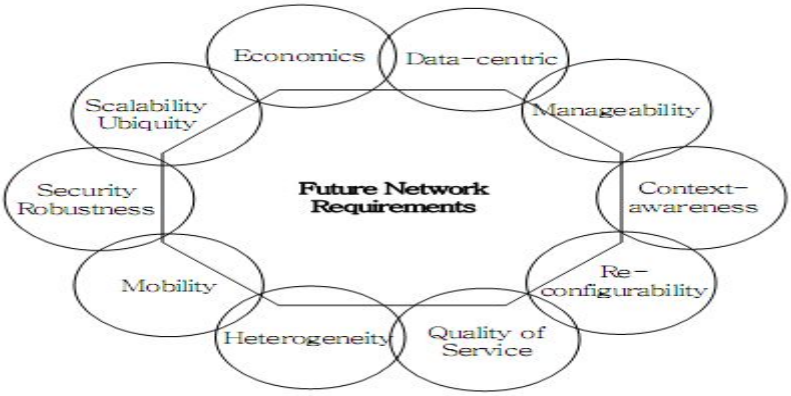
아울러 인터넷 서비스의 양적 증가와 다양성은 참여에 따른 위험을 인지 할 수 없으며 개인정보의 공개 결과를 추적 할 수 없기 때문에 사용자 중심의 개인정보의 통제 수단이 강화될 필요가 있게 된다. 개인정보보호 규제체계는 개인정보를 이용하는 프로그램의 개발을 저해하여 정보 보유자의 혜택 및 비즈니스 공간 발전을 저해 할 수 있기 때문에 적절한 균형이 필요하며, 일상생활에 미치는 영향 증가에 따른 부작용을 막기 위해 사회적 연구와 다양한 사회 집단의 입장을 고려하여야 한다.

경제적 측면에 있어서는 신뢰와 보안관련 연구에 대한 투자가 필수적이며 정보사회에서의 분산된 소유권, 가치향상 등에 대한연구가 필요하며, 데이터 활용에 대한 이해가 부족하기 때문에 비지니스 관점이 요구되고 가치와 분산된 소유권, 가치 향상 등에 대한 연구가 필요하게 된다.

제2절 미래인터넷의 요구사항

미래 인터넷 연구의 등장은 인터넷 혹은 네트워크를 활용하는데 있어 설계 시 고려되지 않은 새로운 형태의 요구가 발생하고 있다. 또한 미래 인터넷이 사용자에게 효과적으로 서비스를 제공하는 기반이 되기 위해서는 사용자가 처한 상황을 정확하게 파악하고 그 상황에 가장 적절한 서비스를 찾아내어 이들 서비스 요소를 실행 중에 서로 연결하고 재구성해 나아갈 수 있어야 한다. 이를 위한 미래인터넷의 설계를 위한 요구사항은 다음과 같다.[11]

11) 신명기, 미래인터넷 기술 및 표준화 동향, ETRI 전자통신동향분석, 2007. 12.



<그림 11> 미래 인터넷 요구 사항

가. 확장성 (Scalability)

확장성은 현 인터넷이 가지고 있는 가장 큰 문제점 중의 하나로 미래인터넷을 설계할 때 가장 중요하게 요구되는 설계 목표 중 하나이다. 먼저 인터넷 대여폭은 앞으로 50~100배 이상 증가할 것으로 예상된다. 또한 미래인터넷은 센서와 같이 새로운 유비쿼터스 단말들이 100억 개 이상 연결되고 천만 개 이상의 멀티홈을 갖는 단말을 지원할 수 있어야 한다. 최근 인터넷은 PI, 멀티호밍, 이동단말, IPv6 영향 등으로 인해 어드레싱과 라우팅 면에서 확장성에 문제가 있음을 보고받고 있다. 따라서 미래 인터넷은 크기, 대여폭, 라우팅, 어드레싱 상에서의 계속적인 인터넷의 증가에 대해 확장성을 갖도록 설계되어야 한다.

나. 보안성/견고성(Security/Robustness)

미래 인터넷은 스팸, 웜, DoS 공격 등 다양한 보안 공격으로부터 완벽하게 안전하다는 것을 전제로 구축되어야 한다. 또한 현재 유선 전화망과 같은 수준의 견고성과 오류 발생 시 복구기능이 제공되어야 한다.

다. 이동성(Mobility)

미래 인터넷은 무선 단말의 이동 시에 이와 연계된 보안과 라우팅 기능이 유선 단말 수준으로 투명하게 이음매 없이 지원되어야 하며, 다양한 물리계층을 지원하는 이기종간 네트워크 환경에서도 빠른 이동성 지원이 제공되어야 한다. 또한 새로운 디바이스로 센서와 RFID와 같은 저 전력, 소형 단말들도 이동성 기능이 제공되어야 한다. 이동 컴퓨팅은 미래 인터넷 응용의 대표적인 사례 중 하나가 될 것으로 전망된다.

라. 이질성(Heterogeneity)

미래 인터넷은 다양한 범위의 새로운 응용들이 지원 가능해야 한다. 또한 광파이버, 다양한 무선링크(IEEE 802.11, 802.16, 802.15.3/802.15.4 등), 애드-혹 네트워킹, 메시 네트워킹 등 이질적 물리 계층을 이음매 없이 지원해야 한다. 이러한 물리 계층의 이질성은 미래인터넷의 이동성 연구, 이기종간 빠른 핸드오버 연구, 프로토콜 계층화 개념에 많은 영향을 미친다.

마. 서비스 품질(Quality of Service)

서비스 품질은 미래인터넷을 위한 새로운 요구사항으로 볼 수는 없지만, 현 IP 기반의 인터넷의 가장 근본적인 제약으로 꼽히는 서비스 품질 제공은 여전히 미래인터넷 설계 목표에서 빠질 수 없는 주요 목표 중의 하나이다. 미래인터넷에서는 다양한 등급의 서비스 품질을 어디에서 어떠한 방법으로 제공해야 하는지에 대한 명확한 구조가 제시되어야 한다.

바. 재설정/자동설정(Re-configurability)

재설정/자동설정 기능은 미래인터넷을 위한 새로운 요구사항 중 하나이다. 현재의 인터넷은 고정적인 네트워크 기능과 장비들로 네트워크로 구성되어 새로운

서비스나 기술들을 적용하기 위해서는 네트워크 토폴로지의 재구성이나 서비스 재설정 등이 동적으로는 불가능하다. 미래인터넷에서는 토폴로지, 장비의 동적인 재설정 등을 제공하기 위해서는 프로그램-가능/자기설정-가능(programmable/selforganized) 네트워킹/컴퓨팅, 네트워크 가상화(networkvirtualization) 방법 등이 적용 가능한 구조로 설계되어야 한다.

사. 상황인지(Context-awareness)

상황인지 기능은 미래 인터넷 서비스를 위한 새로운 요구사항 중의 하나이다. 미래 인터넷 단말들은 잦은 이동에 따른 자신의 물리 환경을 인식하고, 자신이 사용하는 서비스 상황에 맞게 적응할 수 있어야 한다. 상황을 결정짓는 기본적인 요소로는 사용자 위치(where are you), 누구와 있는지(who you are with), 어떠한 자원이 근처에 있는지(what resource are nearby) 등이 사용된다.

아. 관리성(Manageability)

현 인터넷은 관리 플레인(management plane)이라는 개념이 처음부터 설계되지 않았고, SNMP라는 단순한 망 관리 프로토콜을 통해 장비와 네트워크의 오류 등을 모니터링 하는 수준으로 국한되어 관리 기능이 제공되어 왔다. 미래인터넷은 다양한 이기종의 무선, 애드-혹 단말과 네트워크의 빈번한 이동기능 제공이 기본적으로 전제되므로 미래 인터넷에서는 이러한 새로운 환경을 위한 체계적인 관리 기능의 제공이 요구된다. 미래의 이동 단말과 네트워크를 지원하기 위해 관리 측면에서의 편리성, 추적성, 자동성, 최적화 기능 등은 기본적으로 고려되어야 한다.

자. 데이터-중심(Data-centric)

현재의 인터넷은 호스트-중심의 서비스에 맞추어 설계되었다. 대표적인 호스트-중심의 서비스로는 초기, telnet, ftp 응용 등을 들 수 있다. 그러나 P2P와 같이 최근 대두되고 있는 새로운 인터넷 응용들은 사용자가 특정 데이터나 서비스 사

용만을 지정하고, 호스트나 서비스의 위치는 고려할 필요가 없다. 미래인터넷은 이러한 데이터-중심의 새로운 응용이나 서비스 지원이 가능하도록 새롭게 설계되어야 한다.

차. 경제성(Economics)

초기 인터넷은 전문가의 집단에 의해 운용, 사용되어 경제성에 대한 요구사항이 전혀 반영되지 않고 설계된 네트워크이다. 미래인터넷은 ISP나 응용 제공자들이 어떻게 경제적 이익을 창출할 수 있는가에 대한 명시적인 프리미티브를 제공할 수 있어야 한다.

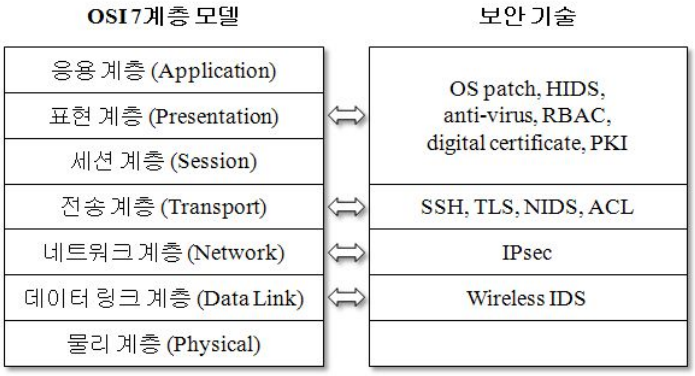
제3절 사이버위협

1. 인터넷 보안의 한계

인터넷의 패러다임은 변화하고 있다. 기존의 '정보 탐색의 도구'에서 지금은 '사회, 경제, 문화생활의 매개체'로 그 역할이 확대되었다. 앞으로 인터넷을 통한 서비스는 더욱 다양해질 것이고, 인터넷은 이러한 새로운 요구조건들을 충족시킬 수 있어야 할 것이다. 현재의 인터넷 아키텍처를 설계한 미국 MIT의 David Clark 교수는 미래의 인터넷은 보안(security), 가용성 및 복원성(availability and resilience), 관리 용이성(manageability), 경제성(economic viability), 지속성(longevity), 사회적 요구(society's needs) 등을 만족시킬 수 있어야 한다고 주장한다. 지금까지 인터넷이 사회의 요구에 부합되도록 눈부신 성장을 해왔지만, 미래에도 그 이상의 역할을 수행하기 위해서는 인터넷이 이와 같은 새로운 요구조건들을 모두 만족시킬 수 있어야 한다.

하지만 현재의 인터넷 아키텍처는 이러한 다양한 요구조건들을 수용하기에 적합하지 못하다. 현재 인터넷은 빠르고 효율적인 데이터 전송을 목적으로 설계되었기 때문에 기본적으로 단순한 구조를 갖는다. 인터넷의 핵심 프로토콜인 TCP/IP

는 데이터 전송에 필요한 최소한의 기능만을 제공한다. 따라서 인터넷은 그동안 새로운 서비스에 대한 요구가 발생할 때마다 이를 만족시키기 위해 OSI 모델의 각 계층 사이사이에 새로운 프로토콜을 삽입하는 형태로 기능들을 추가해왔다. 예를 들어, 안전한 데이터 전송이 필요해짐에 따라 IP와 TCP 헤더 사이에 새로운 IPSEC 헤더를 추가하여 데이터를 암호화했고, 사용자의 이동성(mobility)를 지원하기 위해 새로운 mobile IP 프로토콜을 개발했다. 하지만 이러한 방식의 기능 확대는 인터넷의 복잡도를 증가시키고, 호환성 문제와 같은 부작용을 발생시켰다.



<그림 12> OSI 7계층 모델과 보안 기술의 예

특히, 인터넷 보안과 관련하여 발생하는 새로운 요구조건을 만족시키는 데 한계를 나타내고 있다. 그림 1에서 볼 수 있듯이 대부분의 인터넷 보안 기술들은 응용 계층에 집중되어 있어, 웜, 바이러스와 같은 공격의 경우 일정한 패턴을 찾아내어 호스트 기반 침입탐지시스템(HIDS)과 안티 바이러스 소프트웨어 등으로 어느 정도는 방어할 수 있다. 하지만 네트워크 및 전송 계층의 프로토콜들은 보안을 위한 충분한 정보를 제공하지 않는다. 예를 들어, IP 주소 및 TCP 포트 번호의 변칙 패턴을 이용한 침입 탐지와 같이 간단한 수준의 보안은 가능하지만, DDoS, 봇넷과 같은 대규모의 네트워크 공격에 대한 방어는 현재로써는 불가능하다. 이러한 네트워크 수준의 공격들을 방어하기 위해 지금도 수많은 연구가 진행되고 있지만, 그 누구도 인터넷의 구조적인 한계를 극복하는 근본적인 해결책을 제시하지 못하고 있다.

2. 미래인터넷의 보안 요구사항 및 필요성

현재 인터넷 보안의 한계를 극복하고 미래인터넷을 설계하기 위해서는 설계 초기부터 보안을 고려해야 한다. 인터넷 보안을 위해서 많은 요구 조건들이 있지만 그 중에서도 가장 기본적으로 갖추어야 할 중요한 보안 요구사항은 가용성 (Availability), 추적성 (Traceability) 그리고 프라이버시 (Privacy) 보호 등 세 가지이다. 이들 세 가지는 현재의 인터넷에서는 지원이 안되거나 되더라도 아주 제한적으로만 지원되는 기능들이다. 가용성 확보는 DDoS나 봇넷과 같은 공격 하에서도 서비스를 지속하여 피해를 최소화함을 목표로 한다. 하지만 가용성 확보는 주로 공격이 발생한 후 대처를 원활히 하는 데 초점을 맞추고 있고 공격 원인을 분석한다거나 공격자를 색출하는 것을 목표로 삼고 있지는 않다. 대신 이러한 요구 사항들은 추적성을 확보함으로써 성취할 수 있다. 현재 인터넷에서 가장 구현하기 힘든 보안 요소가 추적성인데, 이는 기존에 이미 구축된 네트워크에 완전한 추적성을 구현하기 위해서는 네트워크 구조 자체를 새로운 형태로 재구축해야 하기 때문이다. 추적성이 구현되면 현재 인터넷 보안의 많은 한계가 극복된다. 다양한 형태로 발생하는 공격의 원인 또는 공격자를 밝혀내는데 핵심적인 역할을 수행할 수 있기 때문이다. 이러한 추적성은 공격의 사후처리에 필수적이지만 합법적인 사용자를 감시하는 데 악용될 수도 있다. 따라서 미래인터넷은 합법적인 사용자를 보호하기 위해서 프라이버시 보호 기능도 제공해야 한다. 프라이버시 보호를 통해 사용자의 개인 정보 및 위치 정보의 유출을 막을 수 있다.

다음에서는 이러한 세 가지 미래인터넷의 보안 요구사항들에 대해 구체적으로 설명한다.

가. 가용성 (Availability)

가용성의 정보보안적인 측면에서의 정의는 허락된 사용자 또는 객체가 언제 어디서나 정보에 접근하려 하고자 할 때 이것이 가능하도록 하는 것이다. 최근에 네트워크의 고도화로 대중에 많이 알려진 서비스 거부 공격 (Denial of Service

Attack, DoS) 이 이러한 가용성을 저해하는 대표적인 공격이다. 현재의 네트워크는 스위치, 라우터 등을 중심으로 한 네트워크 기반구조와 IP, 라우팅 프로토콜 등의 네트워크 프로토콜로 구성되어 있으며, 이들은 원격 호스트들이 패킷을 교환하기 위해 필요한 수단이다. 하지만 이러한 프로토콜과 기반구조는 설계 당시에 가용성을 고려하지 않았기 때문에 원칙적으로 원하는 수준의 가용성을 제공하지 못한다. 이에 따라 현재 인터넷망에서 서비스 거부 공격이 쉽게 가능해졌다. 이러한 예로 지난 2009년 7월 7일에 한국에서 발생한 7.7 대란을 들 수 있다. 한국의 주요 정부기관 및 금융기관을 목표로 분산 서비스 거부 공격 (DDoS) 이 감행되었고, 공격에 활용되었던 DDoS 좀비 PC 들은 소프트웨어적 하드디스크 손상이라는 자기파괴증상으로 증거를 남기지 않았다. 이 사건은 현재 인터넷 상에서 감행된 서비스 거부 공격이 사회 전반에 걸쳐 큰 위협이 됨을 다시 한번 확인시켜주는 계기가 되었다. 이러한 서비스 거부 공격은 점차 지능화, 고도화 되어 가고 있는 추세이며 공격의 양도 증가하고 있다. 따라서 미래인터넷에서도 심각한 위협이 될 것이라 쉽사리 예측할 수 있다.

미래의 서비스 거부 공격은 인터넷의 홈페이지 뿐만 아니라 다양한 모바일 기기도 공격의 대상 또는 경유지로 삼을 수가 있다. 미래인터넷 환경에서는 대부분의 인터넷 사용자가 모바일 기기를 통해 인터넷 접속을 할 것이며, 모바일 기기는 스마트폰, PDA, 넷북 등이 될 것이다. 이 때, 수 많은 기기 또는 PC가 악의적으로 하나의 기지국에 대해서 서비스 거부 공격을 한다면 공격을 받은 기지국이 제 기능을 하지 못하게 되어 그 기지국 영역 안에 있는 많은 사용자에게 서비스를 제공할 수가 없게 된다. 2008년 미국의 한 연구에 따르면 1초에 단 165 개의 sms 메시지로 뉴욕 맨하탄 전체 지역의 셀룰러 망을 마비시킬 수 있다고 한다. 이러한 공격은 가상 시나리오가 아니라 미래에 충분히 일어날 수 있는 공격으로써 대비해야 함을 암시하고 있다.

이러한 서비스 거부 공격은 가용성을 확보하기 위해 네트워크를 이중화, 가상화하거나 또는 경로를 재설정 하는 등의 방법을 동원하여 설계함으로써 어느 정도 경감시킬 수 있다. 가용성을 현재 인터넷에 비해 높게 설계하면 공격자가 서비스 거부 공격을 성공시키기 위해 필요한 좀비 PC의 수나 트래픽의 양이 훨씬 많

아야 할 것이다. 또한 이렇게 많은 수의 좀비 PC나 트래픽을 동원하는 경우 공격의 징후를 미리 발견할 확률이 높아 그에 대한 대비 또한 빨리 할 수 있을 것이다.

이러한 가용성의 확보는 실제로 공격이 일어났을 경우 공격의 피해를 줄이는 방안이 될 수 있지만 공격이 일어난 시점에 공격을 빨리 발견하여 공격자를 추적하고 공격의 근원을 없애는 방법이 되지는 않는다. 이를 위해서는 다음에 소개할 추적성이 별도로 필요하다.

나. 추적성 (Traceability)

미래인터넷이 필수적으로 갖추어야 할 두 번째 보안 요구사항은 추적성이다. 추적성은 책임성 (Accountability) 이라고도 한다. 이것은 정보가 이동할 때 정보의 이동 경로 히스토리나 위치 정보와 같은 신분 정보를 정확히 기록해 놓음으로써 정보가 어디로부터 왔는지를 알 수 있게 하는 것이다. 추적성을 이용하면 공격이 일어난 사후에 공격을 누가 행했는지 그 소스를 추적할 수 있게 된다. 즉 원천적으로 공격의 근원을 알 수 있게 되는 것이다. 하지만 현재 인터넷은 불추적성 (Untraceability)에 기인하여 설계되었기 때문에 많은 공격자들이 자신의 실제 신분이나 위치를 속이거나 노출시키지 않는 상태로 공격을 행하고 있는 실정이다. 이러한 공격 형태는 미래인터넷에서도 큰 위협이 될 것이다. 추적성의 부재로 인해 일어나고 있는 혹은 일어날 수 있는 위협에 대해서 알아보겠다.

첫 번째로 봇넷 (Botnet)을 생각해 볼 수 있다. 스위스 다보스에서 열렸던 세계경제포럼에서 인터넷의 미래를 위협하고 있는 원격조정 사이버 범죄에 대한 경고가 나왔다. 특히 전문가들은 해커의 명령을 원격으로 받아 시스템 정보를 유출시키는 악성 봇에 감염된 PC들의 연결망인 봇넷의 위험성에 대해 주목했다. 원래 봇이란 인터넷 상의 정보 검색을 위해 다른 사이트의 페이지도 자동적으로 연달아 검색 수집하는 프로그램을 일컫는다. 이런 기능이 악용된 악성 봇은 주인 모르게 다른 PC를 마음대로 조정하는 등의 공격을 감행한다. 봇넷에서는 대부분 봇마스터가 많은 수의 감염된 봇을 원격 제어한다. 봇넷의 힘은 매우 막강하다. 왜냐하면 대부분의 봇이 일반적으로 사용자들이 이용하는 개인 PC를 이용하고 외부에

서 볼 때 대부분의 봇이 합법적으로 보이기 때문이다. 이것이 봇넷의 가장 무서운 점이기도 하다. 앞서 언급한 7.7 대란의 서비스 거부 공격도 수많은 일반 개인 PC를 좀비 PC로 이용한 봇넷을 통해 행해진 공격인 만큼 봇넷의 위험도는 상당히 크다고 볼 수 있다. 지금까지의 봇넷은 대부분 IRC를 제어 채널로 이용하였다. IRC는 봇마스터의 입장에서 단순하고 효율적이어서 제어하기 용이하지만 네트워크 관리자 입장에서도 비교적 발견하고 막기가 쉬웠다. 그러나 점차적으로 제어 채널로 IRC가 아니라 Gnutella와 같은 P2P를 사용하는 봇넷이 등장하고 있는 추세이다. 따라서 미래인터넷에서도 P2P 뿐만이 아니라 다양한 프로토콜이 봇넷의 제어 채널로 등장할 것이다. 또한 미래인터넷의 봇넷은 소셜 네트워크를 이용할 가능성도 다분하기 때문에 현재 인터넷에서 보다 더욱 더 큰 위협이 될 것이다. 하지만 미래인터넷이 추적성을 고려하여 설계한다면 문제가 달라진다. 네트워크에서 좀비 PC를 하나라도 찾게 되면 좀비 PC의 제어 채널을 추적하여 봇마스터가 누구인지를 현재에 비해 훨씬 용이하게 찾을 수 있기 때문이다. 봇마스터를 찾게 되면 전체 봇넷을 찾아서 막는 일이 가능해질 것이다.

추적성의 부재로 인해 야기될 수 있는 두 번째 위협으로 스팸 메시지를 생각해 볼 수 있다. 스팸 메시지 기반의 공격에서는 기본적으로 많은 양의 메시지를 다수의 불특정한 인터넷 사용자에게 보내어 특정한 웹사이트에 많이 접속하게 함으로써 특정 상품을 판매하기도 한다. 하지만 최근에는 이러한 단순 판매 뿐 아니라 스팸 메일 자체에 악성 코드가 포함되어 있는 경우가 많아지는 등 중요한 위협으로 부각되고 있다. 전통적으로 스팸은 이메일을 통해 발송되었다. 하지만 최근에는 이메일을 통해 스팸을 보내는 것 뿐만이 아니라 다양한 방법으로 인터넷 사용자에게 보내고 있는 추세이다. 전송 매체의 다각화를 통해 많은 인터넷 사용자에게 스팸을 보내는 방법 외에 새로운 스팸 전송 프로토콜을 개발하기도 한다. 이러한 다양한 방법을 동원하는 이유는 이미 많은 수의 이메일 기반 스팸 필터가 개발되었기 때문이다. 이에 따라 최근에는 이메일 기반의 스팸보다 인스턴트 메시징과 같은 다른 프로토콜을 이용한 스팸이 더 많아지고 있다. 예를 들어, Skype나 MSN 과 같은 인스턴트 메시징 프로토콜을 이용하여 스팸을 보내는 사례가 많아지고 있다. 이러한 메시지는 사용자가 방어하기 훨씬 더 어려운 경향이 있다.

왜냐하면 인스턴트 메시징 서비스는 복잡한 필터링 서비스를 제공하기가 어렵기 때문이다. 미래에는 인터넷에서 사용하는 새로운 통신 프로토콜이 더욱 더 많이 개발될 것이고 스팸은 대부분 그러한 통신 프로토콜을 기반으로 생겨날 것이기 때문에 미래인터넷에서는 현재보다 훨씬 큰 문제가 될 것이다.

결국 미래인터넷에서의 스팸 문제는 더욱 더 정교한 추적성을 요구할 것이다. 추적성이 보장될 수 있는 인터넷 주소 체계가 확립되고 관련 프로토콜들이 정립된다면 메일을 통한 스팸이든 인스턴트 메시징 서비스를 통한 어떤 형태의 스팸이든 모두 다 추적할 수가 있게 되어 보다 안전한 인터넷이 될 수 있다.

세 번째로 나타날 수 있는 위협은 DNS 서버에 기인한 것이다. 현재의 많은 인터넷 어플리케이션은 기본적인 인터넷 라우팅, 네트워크 기반구조와 더불어 DNS(Domain Name Service)를 필수적으로 사용하고 있다. DNS는 IP 주소를 사람이 가독할 수 있는 이름으로 변환해주는 프로토콜이다. 하지만 DNS는 인터넷을 사용할 땐 매우 중요하지만 보안성에 있어서는 아주 취약한 부분이다. 따라서 DNS는 과거에 큰 문제들을 많이 일으킨 적이 있었다. 예를 들어, 해커들은 도메인 이름을 다른 IP 주소와 연결시키는 피싱, 파밍 등의 공격을 하기도 하였고, 합법적인 트래픽을 악의 있는 호스트로 보내는 공격도 하였으며, man-in-the-middle 공격을 시도하기도 하였다. 이러한 종류의 공격을 총칭하여 캐시 포이즈닝(cache-poisoning) 공격이라 하는데 이러한 공격은 최근에 많이 수그러드는 추세였으나 2008년 DNS 구조 자체에 치명적인 결함이 있다는 것을 밝힌 Kaminsky bug 발견 이후 다시 급속도로 증가하고 있는 추세이다. DNS는 이러한 자체의 보안 문제뿐만이 아니라 봇넷과 전자 사기를 위해 남용되기도 한다. 그 중에 하나가 Fast-Flux이다. Fast-Flux는 봇넷에 쓰이는 DNS 공격기술인데 감염된 호스트의 네트워크에 숨어 있으면서 피싱 사이트와 악성소프트웨어 전달 사이트 사이를 돌아다니는 프록시 역할을 한다. 해커는 Fast-Flux를 이용해서 자신만의 도메인 네임을 등록할 수도 있고 도메인 네임과 여러 개의 IP 주소를 연동시킬 수도 있으며 이러한 연동 자체를 쉽게 변화시킬 수도 있다. 이런 방법으로 해커가 만들어 놓은 악의적인 도메인에 일반적인 사용자가 접속하게 되면 실제적으론 봇에 접속이 되는 것이다. 그러면 이 봇은 트래픽을 실제 서버에 포워딩하여

일반적인 사용자는 정상적인 인터넷을 사용하는 것처럼 느껴지지만 실제로는 범죄자가 사용자의 컴퓨터를 직접 제어할 수 있게 되는 것이다. 최근에는 더욱 복잡하고 추적이 힘든 방법으로 사용자와 프록시 사이에 여러 겹의 프록시를 삽입함으로써 악의적인 호스트 위치를 추적하는 것을 훨씬 더 어렵게 하는 방법도 쓰이고 있다. 이러한 DNS 공격 및 Fast-Flux는 미래인터넷에서 더욱 더 활개를 칠 것으로 예상된다. 이러한 DNS 서버를 이용한 공격은 앞서 설명한 위협에 비해 단순히 추적성을 제공함으로써 쉽게 해결되는 문제는 아니다. 하지만 부적절한 IP 매핑이나 Fast-Flux를 발견하게 되면 예전과 달리 미래인터넷에서는 추적성을 이용하여 공격자를 찾게 되므로 공격자가 행한 각종 공격들을 빠르게 파악할 수 있게 되는 것이다.

다. 프라이버시 (Privacy) 보호

앞에서 추적성의 부재로 인해 일어날 수 있는 세 가지 위협에 대해 살펴보았다. 이러한 위협들은 추적성을 통해 억제하고 대응할 수 있으므로 미래 인터넷에서 추적성은 필수적인 보안 요구사항이 된다고 할 수 있겠다. 하지만 추적성은 공격자를 찾는 데는 유용한 요소라 할지라도 합법적인 인터넷 사용자의 프라이버시를 침해할 수 있는 여지를 제공한다. 따라서 미래 인터넷에서는 추적성과 더불어 프라이버시 보호도 제공하여 합법적인 인터넷 사용자의 개인 정보를 보호해야 한다. 프라이버시 보호는 그룹이나 개인의 정보를 선택적으로 격리하여 정보를 보호하는 것을 말한다. 인터넷이 널리 쓰이는 상황에서 프라이버시의 보장은 선택 조건이 아니라 필수 조건이다. 미래 인터넷에서 프라이버시가 보장되지 않으면 다음과 같은 문제가 야기될 수 있다.

첫 번째로 모바일 기기를 통한 개인 정보의 유출을 생각해 볼 수 있다. 미래인터넷에서는 전통적인 연결 기기인 PC나 노트북 외에도 스마트폰, PDA, 보안 카메라, 유비쿼터스 센서 등도 인터넷 연결 기기로 사용될 것이다. 스마트폰은 PC와 같은 기능을 가진 모바일 폰이다. 기본적인 모바일 폰의 기능 뿐 아니라 사용자가 원하는 애플리케이션을 설치하고 사용할 수 있다. 현재에도 스마트폰을 이용하여 이메일, 웹 브라우징, 네비게이션, 음악 감상 뿐만이 아니라 전자 상거래 등도 하

고 있다. 또한 주차시스템이나 대중교통의 결제 수단으로도 이용되고 있는 추세이다. 즉, 모바일 기기에 수많은 개인 정보가 저장되어 있는 것이다. 이러한 상황에서 합법적으로나 불법적으로 추적성을 이용하여 사용자의 모바일 기기에 접속하게 되면, 예를 들어, 주차시스템이나 대중교통 결제 시스템을 통해 사용자의 위치 정보를 얻을 수 있게 된다. 이는 악용될 경우 심각한 사회적 문제를 초래할 수 있다. 또한 전자 상거래 등에 사용되는 공인 인증서나 PIN과 같은 정보를 유출하게 될 경우 피해자가 심각한 재정적인 손해를 입을 수도 있다. 따라서 미래인터넷에서는 프라이버시를 보장하여 추적성이 꼭 필요한 경우가 아니라면 사용할 수 없도록 해야 한다.

두 번째로 다양한 네트워크 환경을 통한 개인 정보의 유출을 생각해 볼 수 있다. 미래인터넷 환경에서는 지금보다 훨씬 다양한 형태의 네트워크들이 구성될 것이다. USN (Ubiquitous Sensor Network)의 사용이 일반화될 것이고, BAN (Body Area Network), CCTV 등도 널리 쓰일 것이다. 이런 환경에서 프라이버시가 보장이 되지 않는다면 유비쿼터스 센서나 CCTV 등을 이용하여 특정 사용자가 어디에 있는지와 같은 물리적인 위치를 쉽게 알 수 있게 된다. 물리적인 위치가 악의적인 목적을 가진 사람에게 유출될 경우 여러 가지 심각한 문제가 발생할 수 있다. 또한 BAN의 경우에, 악의적인 사용자가 특정 인물의 의료 정보를 알아내게 되면 생명에 위협을 가할 수도 있을 것이다. 따라서 미래인터넷에서의 프라이버시 보호는 미래 사회의 요구 조건이며 필수적으로 고려해야할 사항이다.

3. 미래인터넷의 사이버위협

가. 바이러스, 웜 등 악성소프트웨어

먼저 미래인터넷의 큰 위협이 될 악성소프트웨어와 이를 악용한 사기가 위협이 될 수 있다. 예전의 해커들은 단지 재미를 위해 해킹을 했다면 최근의 해커들은 재미 뿐만이 아니라 경제적인 이익을 위해 해킹을 한다. 이러한 추세는 미래인터넷 환경에서 더욱 더 가속화될 것이다. 따라서 해킹을 위한 악성소프트웨어는 더욱 더 증가하고 더욱 더 복잡하고 지능화된 형태로 나타날 것이다. 또한 정교하

고 조직화된 위조로 인해 대규모 범죄가 일어날 확률도 높다. 부수적으로 감염된 호스트 컴퓨터와 개인 정보 등을 매매하는 암거래 시장이 활발해질 가능성 또한 높다.

그리고 기존의 네트워크 인프라구조인 스위치, 라우터 등과 네트워크 프로토콜인 IP, 라우팅 프로토콜 등은 리모트 호스트 들이 패킷을 교환하는 수단을 제공한다. 안타깝게도 이러한 프로토콜과 기반구조는 기본적으로 보안성을 제공하지 못한다. 따라서 호스트 간의 패킷은 쉽게 훔쳐지고 변환될 수 있었다. 잘못된 라우팅 정보를 삽입한다거나, 추적할 수 없는 스팸 발송, 서비스 거부 공격 등이 모두 가능한 것이다. 게다가 패킷을 전송하는 소스는 스푸핑을 통해 누가 보냈는지 속이는 것도 가능하다. 이러한 위협은 현재도 존재하지만 미래인터넷에서도 꾸준한 위협이 될 것이다.

다음으로 DNS와 Fast-Flux가 있다. 많은 인터넷 어플리케이션은 기본적인 인터넷 라우팅과 네트워크 기반구조 뿐 아니라 DNS를 필수적으로 사용하고 있다. DNS는 IP 주소를 사람이 가독할 수 있는 이름으로 변환해주는 프로토콜이다. 하지만 DNS는 인터넷 사용에 매우 중요하지만 사실 보안성에 있어서 매우 취약한 부분이다. 이는 과거에 큰 문제들을 많이 야기시켰다. 예를 들면 해커들이 도메인 이름을 IP 주소와 연결시키거나 합법적인 트래픽을 악의 있는 호스트로 보내고, man-in-the-middle 공격을 하였다. 이러한 캐시 포이즈닝 공격은 최근에 많이 수그러드는 추세였으나 2008년 DNS 구조 자체에 치명적인 결함이 있다는 것을 밝힌 Kaminsky bug 발견 이후 급속도로 증가하고 있다. DNS는 이러한 자체의 보안 문제뿐만이 아니라 봇넷과 사기를 위해 남용되는 문제가 있다. 그 중에 하나가 Fast-Flux 이다. Fast-Flux는 봇넷에 쓰이는 DNS 기술인데 이는 피싱 사이트와 악성소프트웨어 전달 사이트를 프록시처럼 행동하는 감염된 호스트의 네트워크에 있는 소프트기술이다. 구체적으로 Fast-Flux를 이용해서 범죄자는 도메인 네임을 등록할 수 있고 도메인 네임과 여러 개의 IP 주소 사이의 매핑을 자주 바꿀 수 있다. 또한 사용자이후의 프록시 사이에 여러 겹의 프록시를 삽입함으로써 악의적인 호스트 위치를 추적하는 것을 훨씬 더 어렵게 할 수도 있다.

새로운 통신 프로토콜이 보안에 큰 관심을 가져야 되는 또 다른 이유는 봇넷

이다. 봇넷은 자동으로 실행되는 소프트웨어 봇의 집합이라고 생각할 수 있다. 대부분 봇마스터가 많은 수의 감염된 봇을 원격 제어한다. 봇넷의 힘은 막강하다. 왜냐하면 대부분의 봇이 일반적으로 사용자들이 이용하는 개인 PC 이기 때문이다. 그러므로 외부에서 볼 때 대부분의 봇은 합법적으로 보인다. 하지만 지금까지의 봇넷은 대부분 IRC를 제어 채널로 이용하였다. IRC 는 봇마스터의 입장에서 단순하고 효율적이어서 제어하기 용이하지만 네트워크 관리자 입장에서도 비교적 발견하고 막기가 쉬웠다. 그래서 점차적으로 제어 채널로 IRC 말고 Gnutella 와 같은 P2P를 사용하는 봇넷이 등장하고 있는 추세이다. 이러한 현상은 미래인터넷에서는 더욱 더 급속도로 나타날 것이다. P2P 뿐만이 아니라 다양한 프로토콜이 봇넷의 제어 채널로 등장하게 되면 그에 따른 대응 방안도 마련되어야 한다.

새로운 커뮤니케이션 프로토콜에 대한 것으로, 대표적으로 스팸이 이 범주에 들 수 있다. 기본적으로 스팸은 많은 양의 메시지를 인터넷 사용자에게 보냄으로써 특정한 웹사이트에 많이 접속하게 하여 상품을 파는 데 이용되었다. 하지만 최근에는 이러한 단순 판매 뿐 아니라 스팸 메일 자체에 악성 코드가 포함되어 있는 경우도 많아졌다.

스팸은 기존의 이메일을 통해 메시지를 보내는 것뿐만 아니라 최근에는 다양한 방법으로 인터넷 사용자에게 보내진다. 전송 벡터의 다각화를 통해 가능한한 많은 인터넷 사용자에게 스팸을 보내는 방법을 사용한다. 이러한 다각화와 새로운 스팸 전송 프로토콜을 개발하는 이유는 이미 많은 수의 이메일 기반 스팸 필터가 개발되었기 때문이다. 그러므로 이메일 기반의 스팸보다 인스턴트 메시징과 같은 다른 프로토콜을 이용한 스팸이 더 많아지고 있다. 사실 최근엔 Skype 나 MSN 과 같은 인스턴트 메시징 프로토콜을 이용하여 스팸을 보내는 사례가 많아지고 있다. 이러한 메시지는 사용자가 막기가 훨씬 더 어렵다. 왜냐하면 인스턴트 메시징 서비스는 복잡한 필터링 서비스를 제공하기가 어렵기 때문이다. 미래에는 인터넷에서 사용하는 새로운 통신 프로토콜이 더 많이 개발될 것이다. 이러한 스팸은 대부분의 통신 프로토콜에서 생겨날 것이기 때문에 미래인터넷에서는 현재보다 더욱 더 큰 문제가 될 것이다.

나. 스마트 환경

인터넷과 연결되는 기기들이 미래인터넷에서는 기하급수적으로 증가할 것이다. 전통적인 컴퓨터 관련 기기, 스마트폰, PDA, 보안 카메라, 유비쿼터스 센서 등이 될 것이다. 이는 극히 일부분의 예시에 불과하다. 이에 따라 새로운 보안위협이 등장할 것이다.

스마트폰은 PC 와 같은 기능을 가진 모바일 폰이다. 기본적인 모바일 폰의 기능 뿐 아니라 사용자가 원하는 애플리케이션을 인스톨하고 사용할 수 있다. 현재에도 스마트폰을 이용하여 이메일, 웹 브라우징, 네비게이션, 음악 뿐만이 아니라 전자 상거래 등도 하고 있다. 또한 주차시스템이나 대중 교통 수단의 결제 수단으로도 이용되고 있는 추세이다. 이에 비추어 봤을 때 미래에는 이러한 추세가 더욱 더 확대되고 돈과 관련된 컨텐츠가 더욱 더 많아질 것이다. 게다가 전문가들은 미래에 가장 흔한 인터넷 접속 수단으로 모바일 기기를 들고 있다. 하지만 이러한 모바일 기기들은 공격자의 아주 쉬운 먹잇감이 되고 있다. 예를 들어 블루버깅이라는 블루투스의 버그를 이용하여 손쉽게 기기를 장악할 수 있다. 애플사의 iPhone도 이미 장악가능한 상태이다. 그러나 생각해보면 이러한 위협은 PC에서도 똑같이 문제시되었던 것이다. 그러면 이것이 더 큰 문제가 되는 이유를 생각해봐야 한다. 모바일 기기는 PC와는 달리 파워와 물리적인 위치와 관련이 되어있다. 이 두 가지가 심각한 보안 위협을 가져온다.

모바일 기기는 PC와 달리 배터리를 사용한다. 모바일 기기는 최소한의 파워를 사용하여 프로그램을 실행시켜야 한다. 기존의 PC에서 사용하던 보안성이 강화된 애플리케이션은 모바일 기기에서 사용하면 배터리 소모량이 극심하다. 이로 인해 모바일 기기 공급자는 경량화된 애플리케이션을 개발하였다. 경량화라는 의미는 동작만을 위한 기능만 남겨놓고 나머지 기능은 제외했다는 의미다. 여기서 중요한 것은 보안은 나머지 기능에 속한다는 것이다. 즉, 모바일 기기의 사용자와 공급자는 배터리 수명을 위해 보안은 포기했다는 뜻이다.

모바일 기기는 PC와는 달리 휴대하기가 매우 간편하다. 이는 본질적으로 공격자가 훔치기 쉽다는 의미가 된다. 훔치는 것 뿐만이 아니라 잠시 빌려서 데이터를 복사할 수도 있고 프로그램을 설치할 수도 있다. 모바일 기기를 훔치면 공격자

가 공격할 수 있는 옵션이 매우 다양해진다. 공격자는 메모리로부터 직접 데이터를 읽고 쓸 수 있으며 중요한 개인 정보를 빼낼 수도 있다. 또한 더욱 큰 문제는 백도어 프로그램을 설치하여 다시 사용자에게 돌아가면 장시간 사용자의 개인 정보를 빼내기 쉬워진다는 것이다. 또한 공격의 시발점이 어디서든 이루어질 수 있다. 모바일 기기는 어디에나 존재할 수 있기 때문이다.

스마트 환경으로 인해 야기 되는 가장 큰 문제 중에 하나가 미래인터넷에 연결된 센서로부터 들어온 데이터가 믿을 수 있는가이다. 먼저 버그 기기(buggy device)를 문제 삼을 수 있다. 가장 간단한 예를 들면 수퍼마켓에서 바코드 리더가 값을 2배로 올려서 받을 수도 있고, 주차장의 센서가 사용자의 위치를 노출시킬 수도 있다. 이와 같이 잘못된 정보를 읽거나 전달하는 경우가 발생할 수 있다. 그리고 모바일 폰이 공격당해 버그 기기가 될 경우 사용자가 모르는 사이에 전화를 걸 수도 있다. 이로 인해 사용자의 위치 노출 및 전화비 부과 등과 같은 문제가 있을 수 있다.

또 다른 문제로 센서와 데이터베이스가 해킹되는 것을 들 수 있다. 이는 매우 심각한 문제를 초래할 수 있다. 예를 들어 핸드폰 회사의 데이터베이스에 있는 사용자의 정보가 해킹된다면 사용자를 범죄행위와 연관 지을 수도 있고, 쇼핑을 한 것처럼 만들 수도 있다. 즉 가상의 사용자를 복제하는 것이 가능하다는 것이다. 미래인터넷에서 센서의 용도는 기하급수적으로 많아질 것이다. 그 중에 하나가 BAN(Body Area Network)에 사용되는 센서이다. 이는 환자의 생명과 직결된 것이기 때문에 이 센서가 잘못될 경우의 문제는 생명과 관계가 되는 매우 치명적인 것이다.

다. 중요 기반 시스템

치명적인 시스템이라 함은 사회기반시설과 관련된 것들이다. 예를 들면 발전소, 산업 단지, 전화망, 은행망 등을 말한다. 이러한 것들이 인터넷과 연결될 경우에 큰 문제점들이 일어날 수 있다. 가장 큰 이유는 인터넷은 best-effort 패킷 전달 서비스를 기반으로 만들어졌기 때문에 기본적으로 치명적인 어플리케이션과 결합이 쉽지가 않다.

사실 미래인터넷의 위협은 본질적으로 현재인터넷의 위협과 비슷하다. 하지만 스케일이나 방법의 교묘함 등이 현재인터넷 환경보다 훨씬 더 크고 정교하게 나타날 것이다. 여기서 심각한 문제는 미래 환경은 사회전반의 기반 시설의 관리에도 인터넷을 요구한다는 것이다. 즉 인터넷과 중요 기반 시설의 상호의존성에 의해 매우 심각한 문제가 도래할 수 있다는 것이다. 최근 부각되고 있는 스마트그리드와 같은 시스템을 예로 들면, 이는 인터넷과 전력망의 통합을 의미한다. 만약에 전력망에 인터넷을 통해 공격자가 침입하면 피해 정도는 상상 이상이 될 것이다.

중요 애플리케이션에도 마찬가지 현상이 일어날 수 있다. 중요 애플리케이션에서 인터넷을 사용함으로써 애플리케이션의 요구사항과 인터넷과 관련된 컴포넌트 사이에 괴리가 존재할 수 있다. 이 괴리로 인해 컴포넌트의 강인성이 감소될 수 있다. 이는 결국 애플리케이션의 취약성과 위험성을 증가시킨다. 따라서 중요 애플리케이션에서 잘 제어가 되지 않은 인터넷 관련 컴포넌트를 사용하는 것이 새로운 위협이 될 수 있다.

라. 클라우드 컴퓨팅

클라우드 컴퓨팅(Cloud Computing)이란 네트워크에 연결된 전세계 모든 컴퓨터 자원을 흡수해 구름(cloud) 같은 네트워크에 저장하는 것을 의미한다. 따라서 클라우드 컴퓨팅 환경에서는 웹사이트를 비롯해 애플리케이션, 스토리지, API 등이 거대한 유틸리티형 데이터센터에 통합돼 운영된다. 이용자들은 PC뿐 아니라 휴대용 단말이나 전자제품 등의 다양한 단말기를 통해 이 컴퓨팅 자원들에 접근할 수 있다. 즉 개인의 데스크톱 환경, 기업의 정보처리, 인터넷 서비스 등 모든 것이 클라우드 컴퓨팅에 연계되는 것이다. 클라우드 컴퓨팅 서비스가 구현되면 서비스 업체는 모든 자원에 대한 통제권을 갖게 된다. 따라서 클라우드 컴퓨팅 업체는 차세대 서비스 시장을 주도할 수 있는 막강한 힘을 보유하게 된다.

클라우드 컴퓨팅이 활성화되면, 기존에 사용자들이 PC에 저장해 왔던 자료들이 서버 혹은 가상 PC 안에 저장되며, 각종 소프트웨어들을 온라인 환경에서 사용하는 환경이 만들어진다. 가상 환경 기반이므로 작업의 요구 사항에 맞게 자원의 할당이 이루어져 컴퓨팅 환경의 사용 효율은 극대화 된다. 또한 가상 이미지

형태로 사용자 컴퓨팅 환경이 조성되므로 쉽게 이동 가능하고, 가용성도 극대화된다. 사용자 환경을 가상화하여 씬 클라이언트로 서비스하는 것은 이미 몇몇 업체가 구현한 바 있다. 이 경우 활용도가 낮은 PC 기반의 클라이언트에 비해 최소 기능만을 추구한 씬 클라이언트로도 작업 업무 효율을 유지하면서 보안 문제나 관리 문제 등을 해결할 수 있어서 기업 솔루션으로 주목을 받기도 했다. 물론 씬 클라이언트 이외에도 PDA 등의 모바일 장비에서 PC의 환경을 그대로 구현할 수 있다. 플랫폼 독립적인 환경을 위해서 클라우드 컴퓨팅 환경에서는 표준 환경으로 웹 환경을 사용하기도 한다. 운영체제나 하드웨어 종류에 상관없이, 표준을 준수하는 웹 브라우저만으로 사용할 수 있는 환경은 인터넷에 접속되는 디바이스의 종류가 폭발적으로 증가하고 있는 현재 상황에서 플랫폼 독립성과 접근성을 동시에 해결할 수 있는 가장 현실적인 대안이다.

클라우드 컴퓨팅 분야는 아마존이 앞서 나가고 바로 뒤를 구글이 맹추격 중이며, MS와 야후, IBM, 썬 등이 그 뒤를 따르고 있다. 아마존이 아마존 S3 서비스를 시작한 것은 2006년 3월이며, 구글은 2008년 4월에 구글 앱 엔진을 기반으로 한 웹 애플리케이션 서비스를 시작했다. 반면 MS는 아마존 S3와 유사한 데이터 서비스인 'SQL 서버 데이터 서비스'를 2009년부터 제공하겠다고 발표했다. 따라서 클라우드 컴퓨팅 분야에서 아마존은 마이크로소프트에 비해 3년, 구글은 1년 정도 앞선 것으로 평가되고 있다.

IBM은 클라우드 컴퓨팅 개념을 도입한 '블루 클라우드' 프로젝트를 2010년에 상용화 하여 관련 시장에 본격적으로 진출할 예정이다.

썬마이크로시스템즈는 2008년 자바원 회의에서 아마존과 구글이 전개하고 있는 것과 비슷한 '히드라진(Hydrazine) 프로젝트'를 언급했다.

썬의 소프트웨어 담당 부사장은 2008년 안에 아마존의 S3와 유사한 스토리지 서비스를 시작할 예정이라고 밝혔다. 썬은 클라우드 서비스에 이메일과 일정, 메시징 등을 함께 제공할 예정이다.

메이저 IT 업체들의 분주한 움직임 속에서 클라우드 컴퓨팅 시장은 웹 애플리케이션 호스팅 서비스를 중심으로 가속화 되고 있다. 아마존의 AWS와 구글의 웹 애플리케이션 호스팅 서비스가 쌍두마차 체제로 시장을 이끌고 있는 형국이다.

앞으로도 클라우드 컴퓨팅은 IT 전반에 걸쳐 많은 변화를 이끌어낼 것으로 기대된다. 하지만 높은 관심에 비해 아직 클라우드 컴퓨팅을 본격적으로 도입하고자 하는 곳은 많지 않다. 이는 아직 이 기술이 사용자에게 완전하게 신뢰감을 주지 못하고 있다는 것이며, 클라우드 컴퓨팅이 완전히 대세로 자리 잡을지의 여부는 현재 대두된 다양한 문제를 어떤 방법으로 해결할지에 달려 있다. 대표적인 부분이 보안 부분이다. 최근 각종 인터넷 서비스에서 문제가 되고 있는 것이 해킹이나 기타 원인으로 인한 개인 정보의 유출 문제이다. 특히 가상화 기반의 클라우드 컴퓨팅 기반 서비스는 모든 데이터가 서버 쪽에 집중되어 있기 때문에 이 문제에 있어 더욱 위험할 수밖에 없다. 이런 면에서는 지속적인 보안 강화를 통해 사용자에게 신뢰를 쌓을 필요가 있다.

또한 기존의 서버나 메인프레임 등의 전통적인 방식에 비교해 가용성 등에서 확실한 믿음을 주지 못하고 있는 점 또한 개선해야 될 것이다. 물론 이 문제는 기술적인 문제라기보다는 인식의 문제이므로, 앞으로 서비스의 운영에 있어 좋은 모습을 보인다면 이는 자연스럽게 개선이 될 것으로 기대된다. 서비스 중단 등의 문제는 실제로도 종종 일어나고 있다. 얼마 전 구글 앱스 서비스가 몇 시간 정도 장애를 일으키며 거의 사용할 수 없는 상태가 되기도 했고, 그 이전에도 아마존의 클라우드 서비스가 사용 불능 상태에 빠지기도 하는 등의 사례가 있다. 이 경우 심하면 클라우드 컴퓨팅 기반으로 모든 업무를 처리하는 회사의 경우 업무 마비에 빠질 수도 있는 위험한 상황이 된다. 이런 경우는, 클라우드 컴퓨팅의 장점이라는 유연성과 가용성 면에서 문제를 노출시킨 것이다. 분산되어 있지만 하나처럼 동작하는 클라우드 컴퓨팅의 특성을 살려, 좀 더 시스템을 개선할 필요가 있고, 아직 가능성도 충분히 남아 있다. 또한 물리적인 자체 서버 구현에 비해 더 유연하다는 장점은 분명하므로, 앞으로 운영에 대한 경험들이 이런 문제를 해결해 줄 수 있을 것으로 기대된다.

이러한 미래인터넷 환경변화에서 나타나는 위협은 새로운 기기의 등장이나 인터넷환경의 변화로 인해 다양한 형태로 나타날 수 있으나 근본적으로 현재의 사이버 위협과 근본적으로 다른 것은 없다고 할 수 있다.

클라우드 컴퓨팅이나 모바일인터넷 환경 등 미래인터넷 환경에서도 기존의 악

성코드는 지속적으로 나타날 것이며, 스팸메일, 개인정보유출, 사회공학적 해킹, 불건전 정보의 유통, DDoS 공격이나 제로데이 어택과 같은 해킹 등이 대표적인 사이버 위협이라고 할 수 있겠다.

제4장 국내 전문가 설문조사를 통한 미래인터넷의 전망과 위협

미래인터넷에 대하여 국외에서는 많은 연구 프로젝트를 진행하고 논의가 활발하다. 한편 우리나라에서는 아직도 미래인터넷에 대한 연구가 활발하게 이루어지고 있지 못하고 더욱이 미래인터넷에서의 보안의 문제는 아직 걸음마 단계라고 할 수있으며, 점자 연구가 진행되고 있다. 그러나 아직까지도 본격적인 연구가 진행되고 있다고 보기는 어려운 실정이다. 이에 향후 미래인터넷의 변화와 사이버위협에 대한 대응을 알아보기 위하여 국내 보안전문가를 대상으로 미래인터넷의 환경변화와 보안에 대하여 대두시기와 사이버 위협, 대응방안 등에 대하여 설문조사를 실시하였다.

제1절 조사개요

국내 정보보호 관련 전문가 50인을 대상으로 2009년 8월 한달간 관련 설문을 조사하였으며, 24인이 응답을 하였다. 아직까지 미래인터넷에 대한 연구의 부족 등으로 답변에 어려움을 나타내기도 하여 설문회수율은 높지 않다. 전문가 집단의 구성은 정보보호 및 정보통신 관련 기술 분야, 법·행정·사회학, 신문방송 등 사회분야 중 IT 분야 전문가로 구성하였다.

본 설문조사는 향후 다가올 미래인터넷 환경에서의 역기능 이슈와 이에 대한 대응방안을 마련해 보고자 구성된 설문지를 토대로 전문가 의견을 종합 정리하였다. 향후 미래상은 EU의 미래인터넷 보고서를 참조하여 13개의 아이템을 선정하여 각각의 대두시기와 대두되었을 때의 역기능으로 나타날 수 있는 문제점, 이러한 것들이 사회문제화 되는 시기를 예상하고 이러한 문제점을 통해 발생할 수 있는 사고의 영향력 등에 대해 질문하였다. 그리고 이를 해결하기 위한 방안으로 기술적 대응, 법제도적 대응, 사회문화적 대응 등의 우선순위를 파악하고 핵심기술은 무엇이 있는지에 대해 조사하였다.

설문으로 구성된 13개의 미래인터넷 상황은 다음과 같다.

o 인터넷 속도 증가

인터넷 속도가 증가 ('20년에 유선 10G, 무선 1G로 증가예상)

o 인터넷에서의 국가경계 변화

다양한 이기종(유·무선, 센서 등)간의 연결 증가와 인프라 확대로 정보사용자와 저장소의 위치에 따른 문제와 국가간 상이한 규제 및 법률로 인해 분쟁 발생

o 영상, 모션, 소리 등 미디어 데이터 증가

모션 인터페이스 등 다양한 인터페이스와 3D미디어 서비스가 증가

o 심리스(seamless) 환경

사물, 시스템에 내제된 센서등의 통신장치를 통해 시간, 장소에 관계없이 데이터의 저장이나 사용이 끊김없이 지속되는 서비스 환경

o 대용량 데이터의 집적

다수 정보의 수집으로 대용량 데이터의 집적(ex. 휴대폰을 통해 개인의 하루일과 동안 발생하는 음성 및 주변기기의 대용량 정보 수집 가능)

o Internet of Things, Internet with Things

'All IP'의 영향으로 물리적공간의 사물에 내제된 네트워크를 통하여 사물간의 컴퓨팅과 커뮤니케이션 능력이 가능해지며 사이버공간과 소통 원활

o 클라우드 컴퓨팅 환경

저장매체 등이 없이도 컴퓨터 단말 및 이동기기 등을 통해 인터넷 이용

o 개인정보의 경제적 가치 증가

개인정보 및 이동, 사용 이력 상황에 대한 정보등을 수집하고 가공하는 새로운 사업 발생으로 개인 정보의 경제적 가치 증가

o 새로운 웹기반 서비스 경제 활성화

사용자와 판매자 사이의 중간상이 존재가 없어지며 인터넷을 통한 일대일의 소비자 맞춤형 서비스 활성화

o 다양한 ID의 존재

각종 서비스를 이용하기 위한 여러 ID의 사용 증가

o 기술간의 발전속도의 차이 발생

인터넷의 속도, 데이터처리 알고리즘, 데이터의 용량, 저장장치, 보안 등 관련 기술 발전속도 차이발생

o 정보 소통과 통제

기업의 입지 강화를 위해 정보를 독점하려하나 미래 환경에서는 정보소통이 자유로워야 한다. 하지만 정보에 대한 소유권 관리와 통제 필요함

o 소셜 네트워킹의 발전

사이버 공간과 물리적 공간의 경계가 모호해 지고, 사이버 공간의 활동의 증가로 인해 사회적, 윤리적 문제점 발생

제2절 조사결과

1. 미래인터넷에서의 활성화 시기

미래인터넷의 활성화 시기를 예상하는 질문에 전문가 들은 아래와 같이 응답하고 있다. 대두시기를 평균화하여 순위를 정리한 결과이다.

미래인터넷의 활성화는 다양한 ID의 등장이 가장 우선적으로 다가올 변화라고 생각하고 있으며, 개인정보의 경제적 가치가 지금보다 높아진다는 것을 들고 있다. 또한 인터넷의 속도, 데이터처리 알고리즘, 데이터의 용량, 저장장치, 보안 등 관련 기술 발전속도간의 차이가 발생하는 것도 조만간 다가올 변화라고 지적하고 있다.

다음으로 다가올 변화는 웹기반 서비스의 경제의 활성화를 들고 있다. 인터넷 웹을 기반으로 상거래가 활성화 되어 생산자와 소비자가 직접적으로 연결되는 형태가 정착될 전망이다. 그리고 각종 미디어 데이터가 증가하게 되는데 이는 기존의 인터넷을 통해 전달되는 음성, 영상 이외에도 모션데이터를 비롯한 3D 미디어 서비스가 증가하게 될 것이다.

정보소통 통제, 국가 경계의 변화를 그다음 순위로 꼽고 있고 미래인터넷 환경의 큰 변화라고 할 수 있는 클라우드 컴퓨팅 서비스가 그 다음으로 나타날 변화라고 하고 있다. 클라우드 컴퓨팅 서비스는 단말기가 네트워크에 연결되어 사용자들은 지원하는 기술 인프라스트럭처에 대한 전문 지식이 없어도 또는 제어할 줄 몰라도 인터넷으로 부터 서비스를 이용할 수 있는 서비스이다. 별도의 저장장치 등이 필요없이 연결되어 사용자의 데이터를 신뢰성 높은 서버에 보관함으로써 안전하게 보관 할 수 있으며, 기기를 가지지 못한 소외계층도 공공용 컴퓨터나 인터넷에 연결된 컴퓨터가 있다면 개인 컴퓨팅 환경을 누릴 수 있다. 그리고 개인이 가지고 다녀야 하는 장비나 저장공간의 제약도 사라지게 된다.

또한 데이터 용량의 대량화, 소셜 네트워크의 이용 증가, 인터넷 속도 증가, 끊김없는 인터넷 환경을 제공하는 심리스 환경, 사물 간의 커뮤니케이션이 가능해지는 사물인터넷 환경 등이 2015년 중반까지는 나타날 것으로 내다 보고 있다.

< 표 3 > 미래인터넷의 변화상

순위	미래인터넷 변화상	활성화 시기(년)
1	다양한 ID	2010.8
2	개인정보 경제 가치	2011.5
3	기술발전속도 차이	2012.5
4	웹기반 서비스 경제	2012.6
5	미디어 데이터 증가	2012.8
6	정보소통 통제	2013.0
7	국가 경계변화	2013.2
7	클라우드 컴퓨팅	2013.2
9	대용량 데이터	2013.3
10	소셜 Network	2013.4
11	인터넷 속도 증가	2014.9
12	심리스 환경	2015.5
13	Internet Things	2015.6

2. 미래인터넷 환경에서의 사이버 공격유형 및 역기능

조사를 통해서 나타난 미래사회의 역기능으로 가장 많이 지목된 것은 아래의 표에서 나타나듯이 개인정보유출이었다. 개인정보의 유출은 미래인터넷 환경에서 가장 심각히 고려되어야 할 역기능으로 미래인터넷의 주요특징이 개인정보를 활용한 서비스가 다양화 될 전망으로 이에 대한 우려가 가장 높은 것으로 나타났다고 할 수 있다. 자동화된 개인정보의 수집과 이를 활용하는 각종 서비스의 등장으로 경쟁적으로 개인정보를 수집하게 되고 매매행위 등 불법행위가 성행하게 될 것이다. 또한 현재의 개인정보가 개인에 대한 일련의 데이터만을 다루는 것이 아니고 각종 행위 정보나 패턴 정보까지도 해당되어 이를 통해 금전적인 이익을 취하려고 하고 개인은 손해를 볼 우려도 있으며, 프라이버시 침해도 심각한 수준에 이를 것으로 보인다.

다음으로 우려하는 것이 사회공학적 해킹이다. 사회공학적 해킹은 시스템이 아닌 사람의 취약점을 공략하여 정보를 얻어내는 공격기법을 통칭하고 있다. 불확실

성이 내포되어 있는 보안대책은 취약성을 지닐 수 밖에 없음을 고려할 때 많은 변수를 가지고 있는 인간이라는 요소는 시스템 내에서 취약점으로 작용할 수 있다. 이러한 예는 전화사기나 이메일 피싱, 우편물 등을 통해 개인정보를 도난 당하고 특별한 기술 없이도 손쉽게 기본정보를 얻어애는 비기술적 침해 유형이다. 인간 상호작용의 신뢰를 바탕으로 사람을 속여 정상적인 보안절차를 무력화시키고 원하는 정보를 탈취하는 기술로 공격대상에게 신뢰를 줄수 있는 위장, 가장을 통해 공격자가 접근시 보유한 정보의 가치에 대한 무지, 보안의식 부재 등은 사회공학적 공격에 대한 취약적으로 작용한다.

다음으로 최근 발생하여 커다란 피해을 입힌 분산서비스 공격{Distribute Denial of Service attack, DDoS)공격이 있다. 여러 대의 컴퓨터를 일제히 동작하게 하여 특정 사이트를 공격하는 해킹 방식의 하나로, 한명 또는 그 이상의 사용자가 시스템의 리소스를 독점하거나, 파괴함으로써 시스템이 더 이상 정상적인 서비스를 할 수 없도록 만드는 공격 방법이다. 이는 특정 컴퓨터에 침투해 자료를 삭제하거나 훔쳐가는 것이 아니라 목표 서버가 다른 정당한 신호를 받지 못하게 방해하는 작용을 하게 되며, 대량의 접속을 유발해 해당 컴퓨터의 기능을 마비시키는 수법이다.

제로 데이 공격 또는 위협은 알려지지 않은 위협이나 취약점을 이용하여, 패치가 필요한 프로그램을 악용하여 공격하는 사이버 상의 공격이다. 제로 데이 공격 대상물이 되는 프로그램은 예방프로그램을 개발하기 이전 즉 공식적인 패치가 배포되기 전에 최근 발견한 취약점을 이용하 공격하는 것으로 이런 프로그램들은 보통 대중들에게 공개되기 전 공격자들에게로 배포된다.

최근의 해킹은 웹사이트를 공격하는 형태가 두드러지고 있으며, 자동화된 툴을 이용해서 대량으로 웹해킹이 일어나고 있다. 향후에도 웹2.0 등 웹의 이용이 지속적으로 늘어날 것이며, 서비스이용자는 웹사이트를 통해 거의 모든 정보를 얻고 정보를 제공하여 웹의 해킹으로 인해 각종 데이터가 유출 될 수 있다. 웹해킹에서 가장 우려되는 것은 전통적인 보안 솔루션으로는 막기 어렵다는 것이고, 웹 서비스는 누구든지 항상 접근이 되어야 하며, 웹해킹으로 웹페이지에 악성코드나 악성 프로그램 삽입이 되었을 경우 해당 웹페이지에 접근하는 사용자가 피해를 입을

수 있다는 것이다. 웹서비스를 이용하는 이용자의 개인정보 유출의 원인이 되며, 기업입장에서는 신뢰를 떨어뜨려 사업에도 영향을 미칠 수 있게된다.

컴퓨터 바이러스는 컴퓨터 프로그램이나 실행 가능한 부분을 변형하여, 여기에 자기 자신 또는 자신의 변형을 복사하여 컴퓨터 작동에 피해를 주는 명령어들의 조합을 일컫는 것으로 단순한 데이터의 증가를 통해 피해를 입히는 형태에서 자기복제를 통해 퍼져나가면서 컴퓨터 내의 정보를 빼내가는 형태로 지속적인 진화를 거듭하여 왔다. 바이러스 뿐만아니라 웜이나 트로이목마와 같은 악성코드가 활개를 치고 현재는 악성코드별로 영역조차 구분하기 힘들 정도로 복합적인 면을 보이면서 신종 악성코드가 증가하고 있는 상황이다. 향후에도 가장 많이 쓰이는 플랫폼을 중심으로, 즉 공격하기 쉬운 형태의 대표적인 악성코드가 유행할 것으로 보인다.

이밖에도 인터넷 미디어의 발달 등으로 불건전정보 유통이나 스팸메일도 갈수록 증가할 것이며, 다양한 형태로 나타날 전망이다. 특히 악성코드 등이 스팸메일을 통해 유통되고 불건전 정보를 다루는 사이트를 통해 유통될 가능성이 존재하여 이에 대한 대비가 필요할 것이다.

<표 4> 사이버위협 및 역기능에 대한 응답 빈도 (단위: 응답수)

사이버 공격	인터넷 속도 증가	인터넷에서의 국가경계의 변화	미디어 데이터 증가	심리스 환경	대용량 데이터의 집적	Internet of Things	클라우드 컴퓨팅	개인정보의 경제적 가치	새로운 웹기반 서비스	다양한 ID 존재	기술간 발전속도의 차이 발생	정보소통과 통제	소셜 네트워킹의 발전	계
개인정보 침해	10	13	8	16	16	7	14	21	9	15	5	13	13	160
사회공학적 해킹	9	10	5	7	6	7	7	9	9	10	5	6	16	106
DDoS 공격	20	5	5	8	1	13	12	-	7	1	10	-	2	84
바이러스 웜	14	8	7	12	6	9	7	4	4	1	8	-	4	84
웹공격	13	4	1	2	2	6	10	1	11	3	7	1	4	65
불건전정보유통	10	5	12	2	1	3	2	2	5	2	3	4	6	57
제로데이 공격	11	6	4	4	2	5	7	1	3	-	11	-	2	56
스팸메일	9	5	6	2	4	3	2	1	7	6	4	-	2	51

이밖에 기타의견으로는 새로운 웹기반 서비스의 이용에 따라 인터넷 사기가 극성을 부릴 것이며, 다양한 ID가 나타나면서 ID 도용과 이것이 악용되어 명의도용에 까지 이를 수 있다는 것이다.

미래사회에 각각의 기술간 발전속도의 차이를 보이면서 기술간 발전속도 차이 자체가 역기능이 될 수 있으며, 기업의 정보가 유출 될 우려를 나타내고 있고 기술의 발전과 개인의 정보처리능력 간의 격차가 확대될 우려가 있다.

정보소통과 통제 환경에서는 저작권의 침해라든가 정보의 독점이 나타날 수 있으며, 소셜 네트워킹의 발전으로 인해서는 인터넷 중독과 정체성의 혼란, 그리고

소셜 네트워킹 서비스를 통한 편향적인 여론의 독점이나 정치적 악용 등의 우려도 나타내고 있다.

3. 미래인터넷 환경에서의 사이버 공격유형 및 역기능에 대한 대응

조사대상 전문가들은 미래인터넷 환경에서 예상되는 역기능에 대한 대응방안으로 다음과 같은 의견을 제시하고 있다. 미래환경변화에 따른 대응방안으로 정리하도록 하겠다.

1) 인터넷의 속도 증가

인터넷의 속도증가로 인한 사이버 위협에 대한 대응으로는 인식제고 등 사회적 대책 강화가 가장 우선적으로 해결해야 할 과제로 응답하고 있었으며, 기술적인 대응도 중요한 대응이라고 응답하고 있다. 그리고 추가적으로 인터넷사용 윤리 강화, 기업의 마케팅을 위한 무분별한 개인 정보 이용제재, 정보윤리 기준의 법 제도 강화, 새로운 인터넷 문화 구축, 건전문화 정착홍보, 인간의 삶이 윤택하기 위해서 건전한 사용을 가능하게 하도록 해당 서비스의 활성화 및 법제도의 개선, 사이버 공간도 책임을 져야 하는 공간이라는 인식제고, 사이버범죄 인식 제고 및 대안 공유 및 방지책 확산, ID도용방지, 신원확인 시스템 등 소셜 네트워킹 정보보호 가이드 구축, 소셜네트워킹 사이트 이용자들에 대한 디지털 시민윤리 교육 및 인터넷 윤리교육 강화 등의 의견이 있었다.

이에 필요한 구체화된 기술적인 요소로는 시스템의 분산운영, 악성코드 대응 및 경량 암호기술, 네트워크 보안 장비 개발, 차세대 인터넷 보안 프로토콜 개발 및 암호화 알고리즘 개발, 다양한 인터넷 방식의 보안성 있는 호환 기술, 신규 바이러스나 웜의 탐지기술, 보안 관리 프로토콜, 사이버공격 탐지 기술, 네트워크 대역폭의 증가로 인한 역기능에 대한 모니터링 및 대응을 위한 기술 개발을 들고 있다. 또한 실시간 DDoS 대응 기술, 사용자 측면에서의 개인정보보호 기술, 능동적 위험관리 방안 및 기술, 인터넷 프로토콜의 보안, 사이버공격을 중단, 차단하기 위한 가상PC 혹은 가상 웹서비스가 필요하고, 속도가 빨라지는 만큼 해킹 속도가

빨라질것으로 예상되어 속도를 고려한 해킹 예방기술이나 해킹에 대응할 수 있는 ID 관리(Identity Management) 기술의 필요성을 지적하고 있다.

2) 인터넷에서의 국가경계 변화

인터넷의 국가경계의 변화에 대한 사이버 위협의 대응으로는 규제 중심의 법제도가 시급한 문제라고 지적하고 있으며, 유무선 융합, 통합 메시지등 차세대응용서비스에 적합한 보안기술개발, 범죄자 인도조약 강화, 국제 규약 체결, 한국인터넷 환경을 고려한 세계 인터넷 표준화, 국가간 협조문 작성 등이 필요하며, 적대적 정보유출과 불건전 정보 유통에 대응하기 위한 국가적 협력이 요구된다고 한다. 아울러 국가간 보안정보 공유체계 마련, 국제 표준/지침/가이드라인 연구 및 적용방안 최적화, 정부를 비롯한 업계, 직무 등 다양한 수준에서의 IT Compliance 확립 등이 필요하다고 하고 있다.

또한 이를 위한 주요 정보보호 기술로는 이기종 간 융합에 따른 보안인프라 개발, ID 관리 기술, 통합인증 기술, 사이버 범죄 위치 추적, 국제 정보보호 거버넌스 체계구축, 세계의 인터넷 규제 및 법률 표준화, 공조체계 문서화, 보안 관련 국제 표준 채택 및 적용, 침해사고 협력 프로토콜, 개인정보 유출들이 이루어지는 맬웨어에 대한 유포추적을 위한 기술이 요구되며, 정보보호 정책 협상 및 표현 기술, 국제 규범, 가이드라인에 준하는 개인정보 공유 및 관리 방안, 이기종 융합 서버 및 스토리지에 대한 ERP차원에 통합적/전사적 리스트 관리 시스템, 스팸차단 기술, DDoS공격대응 기술 역추적, 국제적 협력 방안 마련 등이 필요하다고 지적하고 있다.

3) 영상, 모션, 소리 등 미디어 데이터 증가

모션 인터페이스 등 다양한 인터페이스와 3D미디어 서비스가 증가할 것이다. 이에 대해 전문가들은 기술적인 대응이 필요하다고 응답하고 있다.

이에 필요한 대응방안으로는 대용량 미디어를 효율적으로 보호할 수 있는 보안 기술, 새로운 종류의 개인정보인 생체데이터, 위치데이터 등과 관련된 보호정책

책정, 컨텐츠 암호화, 불정당한 데이터 배포자 추적기술 개발, 사용자 인증 기술 개발, 새로운 미디어 데이터에 대한 처벌 및 벌금 제도 적용, 고성능 프로토콜 개발, 다양한 인터페이스에 대한 활성화 유도와 동시에 안전한 대책에 대한 의무화, 유해물의 위험에 대한 정규 교육, 컨텐츠 보호 및 저장, 공유, 이기종 미디어 영상 통합 운영, new 인터페이스 기반의 미디어 데이터 보호가 필요하다고 한다.

또한 이를 위해 필요한 기술적 요소로는 미디어 관련 보안기술 개발, 멀티미디어 암호화 기술, DRM, 개인정보보호기술, 멀티미디어 융합보안 기술 개발, 컨텐츠 암호화 및 사용자 인증, 무단복제 방지기술, 웜 바이러스 대응 기술, 불건전 정보 탐지 및 차단기술, 새로운 스트림 서비스와 새로운 인터페이스를 이용한 역기능에 대한 대응 기술, 스트림 기반의 DDoS, 새로운 인터페이스를 이용한 웜 전파 등 유해물 차단 및 저작권 보호기술, 이기종 다매체 통합운영 서비스 및 지원 기술, 기존의 멀티미디어 데이터 보안시스템 더욱 강화한 데이터 보호체계 구축이 필요하다고 한다.

4) 심리스(seamless) 환경

사물, 시스템에 내제된 센서 등의 통신장치를 통해 시간, 장소에 관계없이 데이터의 저장이나 사용이 끊김없이 지속되는 서비스 환경을 구축할 수 있다.

이에 대한 주요 대응으로는 기술적인 대응이 우선시되며, 심리스 환경에 적합한 보안 기술, 봉인 확인을 통한 자료의 열람이 가능하도록 제한하거나, 홍채인식·지문인식 등의 생체정보 인식 시스템, 성문과 정맥 확인 기법, DDoS 탐지 기술, 데이터 암호화, 사용자 인증, 품질보장 관점의 심리스한 서비스 보안 기술, 통합 식별 및 인증 기술, seamless computing 환경에 적합한 사용자 인증시스템, 사용자 중심의 개인정보보호 기술 등이 요구된다.

또한 필요한 정보보호 기술로는 센서 네트워크 보안, 기기인증 기술, VPN, 경량 암호, DRM 본인 확인 시스템, DDoS 예방 및 탐지, 데이터 비화 기술, 센서통합보안체계, 보안연속성 보장을 위한 기술, 논리적/물리적 심리스 인증 기술, 이기종 다매체 통합 디바이스 연동 기술 및 서비스 인프라 확립 기술, 이기종 기기간의 해킹 방지, 서비스거부공격방어, 개인의 Privacy 보호를 위한 blocker-tag 기반

의 protection tool 개발 및 보급, 바이러스/웜 오토자가진단 시스템, 셀프-프로텍션 기술 등이 필요하다고 하고 있다.

5) 대용량 데이터의 집적

대용량 데이터의 집적으로 인한 정보보호 대응방안은 수집 주체, 수집 기술에 대한 통제, 개인휴대단말에 대한 정보 보안 기술, 봉인 확인을 통한 자료의 열람이 가능하도록 제한하거나 생체정보 인식 시스템 및 성문과 정맥 확인 기법, 새로운 데이터 암호화, 사용자 인증, 프라이버시를 고려한 데이터 처리 기술 및 안전한 개인정보 저장 및 관리 기술 개발, 컨버전스 서비스 및 비즈니스 융합 관련 제도 및 전문가 양성, 휴대폰/USB 등 사용자 중심의 접근제어 기술개발 및 보급, 사용자들의 대용량 파일 공유 및 관리에 대한 안전교육 등이 필요하다.

또한 필요한 정보보호 기술로는 DATA에 대한 접근통제 기술, DB 보안, 디스크 등 미디어 보호, 접근 제어, 본인 확인 시스템, SANS 보안 시스템 구축, 데이터 암호화, 사용자 인증, 간편하고 강력한 본인 인증 기술, 데이터 전송 암호화, 개인정보 등 수집정보에 대한 활용의 투명성 보장을 위한 기술 및 자율적 개인정보 제어를 위한 기술 개발, 프라이버시 보장형 데이터 마이닝 기술 및 휴대단말분실 및 손망실시 개인정보 보호 기술, 역학 기반의 접근제어 고도화, 클라우드 컴퓨팅 보안 기술, 정보의 신뢰성 있는 관리 기술, 개인정보 암호화, 사용자의 대용량 데이터 보호 및 관리가 보장되는 가상화 데이터 센터 구축 및 유무선 통합 방화벽 강화, 개인정보보호 등 정보보호를 위한 네트워크 프로토콜 개발 등이 있다.

6) Internet of Things, Internet with Things

'All IP'의 영향으로 물리적공간의 사물에 내제된 네트워크를 통하여 사물간의 컴퓨팅과 커뮤니케이션 능력이 가능해지며 사이버공간과 소통 원활이라는 측면에서 정보보호의 대응과 필요기술에 대한 설문에 대하여 다음과 같이 응답하고 있다.

환경에 적합한 보안 기술이나 사물의 오작동을 관리할 수 있는 시스템을 구축

하고 해커에 의한 가전제품의 오작동으로 인한 피해방지, DDoS 탐지 기술, 새로운 바이러스나 웜의 탐지기술, 새로운 인터넷 환경의 보안 위험성 인식 교육, 이기종 연동 기술 개발, 위치정보 관련 법률 확대, 모든 개체들에 대한 통합 ID 관리 플랫폼 기술개발 필요, 시간과 장소 불문하고 개인 정보보호가 일상화, 내면화될 수 있도록 유비쿼터스 정보보호 및 보안교육의 강화가 필요하다고 한다.

또한 필요한 기술로는 IPv6 보안 기술, 디바이스 인증, 접근제어보안기술로 네트워크 U-보안 시스템 구축, 새로운 바이러스/웜 공격의 예방 및 탐지 기술, 사용자 인증, 유무선 복합 연동 기술 개발, 위치 정보 보안 기술, M2M 통신용 인증인가, 신뢰기반의 사물통신을 위한 디바이스 인증 및 컨텐츠 인증을 위한 기술이 요구되며, 사물간의 신뢰관리 기술 및 인증과 ID관리기술, 사이버공간 내 Reallity 융합 및 운영관리 기술, 유무선 통합 네트워크 및 관련 다매체제어 기술, 기기내의 system보안 기술, 시스템오작동 실시간 진단 장치, 개인의 위치정보 추적, RFID 위변조 및 복제, 도청 등을 방지할 수 있는 정보보호기술이 중요하게 부각될 것으로 예상하고 있다.

7) 클라우드 컴퓨팅 환경

저장매체 등이 없이도 단말기만을 이용해서 인터넷을 이용할 수 있는 환경인 클라우드 컴퓨팅 환경에서는 네트워크에 저장된 정보의 보호나 제3자에게 정보의 노출을 금지시키거나 데이터 미러링을 통한 안정성 강화, 서버보안 강화, 클라우드 환경에 적합한 데이터 암호화, 사용자 인증, 데이터 보호 및 관리에 대한 규제 등의 클라우드 컴퓨팅 제공자가 준수해야할 법적 제도의 표준화가 필요하다고 한다. 이밖에도 데이터소유의식 변화나 개인정보의 집중화된 서버의 관리가 강화되는 구조이므로 이와 관련한 불법적인 활용에 대한 책임의무의 강화가 요구되며, ownership의 정립과 책임의 명확화, 안티바이러스・안티스팸 등 다양한 레벨의 보안기능을 제공하는 통합적 보안시스템 및 스마트 디펜스 체계구축, 클라우드 컴퓨팅의 보안 취약성에 대한 관리강화를 위한 규제체계 확립이 필요하다고 한다.

다음으로 필요한 정보보호 기술로는 연결된 정보에 대한 침해피해를 방지할 수 있는 기술, 접근제어 관리, 가상 OS 보안, 접근 통제, 인증 및 암호화 기술, 대

용량 데이터 암호 기술, 클라우드 컴퓨팅 전송데이터 암호화, 단말기 인증기술, 사용자 편리성과 보안성을 강화한 인증기술, 협업 환경 내 접근제어 및 데이터 보안 기술 고도화가 필요하며, 클라우드 컴퓨팅 그 자체로 정보보호를 원천적으로 가능케 하는 new 클라우드 컴퓨팅 서비스 개발이나 네트워크 보안기능 강화, 개인정보보호 침입탐지시스템 등이 필요하다.

8) 개인정보의 경제적 가치 증가

미래인터넷 환경에서는 개인정보 및 이동·사용 이력 상황에 대한 정보 등을 수집하고 가공하는 새로운 사업의 발생으로 개인 정보의 경제적 가치가 증가하게 된다. 이러한 개인정보의 경제적 가치에 대한 정보보호 대응방안으로는 정보의 수집 및 가공에 대한 통제, 개인정보 암호화 및 관리의 강화, SSL 방식의 암호화 정보 전달, 개인정보 관리규제의 강화, 사용자 인증, 기업의 데이터 관리에 대한 법적 규제, 데이터 침해 및 도용 등에 따른 벌금 및 처벌 제도 확립, 범죄행위로 인식변화, 개인정보에 대한 지식화에 따라 이의 활용에 대한 책임 및 법적 의무에 대한 강화가 필요, 개인정보 자기통제권 강화 기술 필요, 개인정보의 침해에 대한 강화 처벌 및 합법적인 이용을 보장 할 수 있도록 법규 정비, 분산된 개인정보 보호에 대하여 이용자 측면의 개인정보 보호법 입법의 필요성, 개인정보의 무단사용 및 가공을 통한 경제적 이득추구 행위에 대한 법적 규제 강화, 사용자 개인의 정보관리 의식 강화를 위한 교육체계 마련 등이 있다.

또한 필요한 기술로는 대용량 데이터의 암호 기술, 익명성 보장 기술, 개인정보 영향평가 기법 개발 및 가치산정기법 개발, 사용자 인증, 접근제어, 온라인 행동(타켓)마케팅 보안 기술, 개인정보 자기 통제권을 제공하기 위한 기술 개발이 요구되며, 개인정보의 오남용을 방지하기 위한 인증서비스, 저장매체 등의 안전삭제 시스템 등 개인정보 침해여부 실시간 확인 기술, 전자서명 개인정보에 대한 사용료 지급 근거가 되는 접근기록/보존 등이 필요하다.

9) 새로운 웹기반 서비스 경제 활성화

사용자와 판매자 사이의 중간상이 없어지며 인터넷을 통한 일대일의 소비자 맞춤형 서비스 활성화가 이루어질 것이며, 이에 대한 정보보호 방안으로는 보안기술에 기반한 판매 사이트 인증제도, 해킹에 대처할 수 있는 기술 강화, 비정상 패킷 탐지 및 필터링·탐지 기술, DDoS 예방 및 탐지 기술, 새로운 인터넷 문화 구축, 새로운 경제활동으로 인식, 새로운 웹기반 서비스 경제 활성화를 위해서는 신뢰 할 수 있는 인프라 구축이 우선되어야 하며 이를 위한 법제도적인 보완이 요구되며, 웹기반 전자상거래 서비스에 대한 사용자의 신뢰 및 평판 시스템 활성화 지원이 필요하다.

필요한 정보보호 기술로는 웹방화벽, 피싱 방지 기술, 웹 2.0 기반 보안 시스템 구축, 비정상 패킷 탐지 및 필터링 기술, 부인방지 기술, B2C 보안 기술, 모바일 지불 결제 및 이용자중심의 개인정보 공유 제어 기술, Collaboration 환경내 비즈니스 변화에 따른 패러다임, 인지에 따른 Secure e-marketplace 적용 보안 기술 및 통제 등이 필요하다.

10) 다양한 ID의 존재

각종 서비스를 이용하기 위한 여러 ID의 사용 증가에 대한 정보보호 대응 방안으로는 기존 ID 관리 기술의 활성화 유도, 중복 가입 방지를 위한 개인 확인 시스템 개발, 주민등록번호 확인 및 주민번호 대체수단의 적용, 새로운 인증 기술 개발, 새로운 인터넷 문화 구축, 익명인증 등 제도 지원이 필요하며 대체 ID 활성화, 공공행정정보 이용시 단일 ID 등 통합적 인증, 무분별한 ID 남용방지를 위한 의식교육 강화, 인터넷 정보 보안 교육 강화가 필요하다.

또한 필요한 정보보호 기술로는 사용자의 편의성을 보장하기 위한 강력하면서도 간편한 통합 식별 기술 개발, 사용자중심의 ID관리 기술, 통합 ID 관리 기술, ID 관리 기술, 전자지갑 등 통합된 ID 관리 시스템 개발, 새로운 인증 기술 개발, 생체인증, OTP 등 복합기술의 개발, ID 융합 보안기술, 온오프라인 연계형 통합 ID관리 기술, CMS-Consolidated ID Management Solution, 개인정보보호, ID도용

방지를 위해 여러 개의 객체 식별자를 가지도록 신원확인 및 암호알고리즘을 더욱 정교화하는 서비스, 주민번호 대체수단의 활성화, Identity Management 암호응용기술 생체 인식기술 등이 필요하다.

11) 기술간의 발전속도의 차이 발생

인터넷의 속도, 데이터처리 알고리즘, 데이터의 용량, 저장장치, 보안 등 관련 기술 발전속도 차이발생에 대한 정보보호 대응방안으로는 기술 격차를 줄일 수 있는 보안 기술 개발, 기술간 균형 발전을 위한 투자 및 정책 마련, 보안 관련 업체 중 우수업체를 선정 하는 등의 노력, 화이트 해커 양성을 통한 보안 기술 발전 도모, 기존 기술 방식과 호환되는 보안 기술 개발, 자율경쟁 지원이 필요하며, 네트워크 및 서비스의 발전 속도에 비하여 정보보호 기술의 고성능화가 많은 지연을 보여 이에 대한 고성능 보안기술 개발이 필요하다. 다양한 보안 정책과 시스템이 상호운영 가능한 체계, 기술들간의 성장격차를 조절하기 위한 거버넌스 구축, 격차의 구조화로 인해 잠재적 발전가능성이 발현되지 못하는 기술에 대한 효과적 지원강화가 필요하다.

또한 필요한 정보보호 기술로는 보안기술의 고속화, 경량화, 데이터베이스 보안, 프라이버시 보호, 기술격차 해소를 위한 산업육성 및 지원, 여러 장치와 기술간 호환 가능한 보안 기술, 각 분야의 지속적 성능개선, 네트워크 레벨에서는 고성능 데이터 센싱 분석, 보안 정책 협상 기술 및 TIP 기반 인증 기술, WEB INTERFACE Control 및 Monitoring 기술, 기술의 발전속도에 따라 연동 발전하는 정보보호 서비스 및 규칙제공, 전자서명 이용활성화 등을 들고 있다.

12) 정보 소통과 통제

기업의 입지 강화를 위해 정보를 독점하려하나 미래 환경에서는 정보소통이 자유로워야 한다. 하지만 정보에 대한 소유권의 관리와 통제가 필요하며, 정보 소통의 중요성을 인식시키고, 정보관리에 대한 법적 규제를 강화시켜나가야 하며, 사회적 신뢰성 회복을 위해 노력해야 한다는 것이다. 부당한 개인정보 침해를 막기

위한 개인정보 활용에 대한 강력한 책임과 의무를 부과하기 위한 법제도가 개선되어야 하며, 불법 콘텐츠 유통이 범죄라는 인식을 확산하는 것이 필요하다. 정보의 제어, 유통, 공유에 대한 명확한 가이드라인 및 통제 방안이 확립되어야 하고, 특정기업에서의 정보독점이 두드러질 것으로 예상 되어 이에 대한 정보독점 규제 체계를 확립해야 할 것이다.

이러한 대응을 위해서 필요한 기술적 요소로는 데이터베이스 보안, 프라이버시 보호, 정보보호 거버넌스 체계 구축과 제도화 추진, 정보관리 시스템 통제 기술 등이 필요하며, 웹 2.0의 확대 적용, 정보에 대한 소유권 관리와 자기정보 통제를 위한 기술의 성숙이 요구된다. 저작권 관리 및 유통 기술, 속성 인증기술과 정보제어 기술의 활성화 및 통합 보안 기술, 사용자가 스스로 자신의 개인정보를 보호관리하는 솔루션 서비스 제공, 워터마킹 등이 필요하다.

13) 소셜 네트워킹의 발전

사이버 공간과 물리적 공간의 경계가 모호해 지고, 사이버 공간의 활동의 증가로 인해 사회적, 윤리적 문제점이 발생하게 된다. 소셜 네트워킹의 경우 특히나 기술적인 대응보다는 사회문화적인 대응이 요구되고 있는데 인터넷 사용윤리를 강화하고 기업의 마케팅을 위한 무분별한 개인 정보 수집 및 이용을 제재할 수 있는 수단을 강구해야 하며, 정보윤리 기준의 법제도를 강화하고 아울러 건전한 인터넷 이용문화를 구축하고 이를 홍보해 나가야 한다.

즉, 인간의 삶이 윤택하기 위해서 건전한 사용을 가능하게 하도록 해당 서비스의 활성화 및 법제도의 개선이 요구되며, 사이버 공간도 책임을 져야 하는 공간이라는 인식제고가 필요하며, 사이버범죄 인식 제고 및 대안의 공유와 방지책을 확산 시켜야 한다. 아울러 ID도용방지, 신원확인 시스템 등 소셜 네트워킹 정보보호 가이드라인을 개발하고 소셜네트워킹 사이트 이용자들에 대한 디지털 시민윤리 교육, RBAC(Role Based Access Control) 인터넷윤리 교육 등 인터넷 윤리교육을 강화해 나가야 한다.

구체화된 기술적인 요소로는 비윤리적 정보 교화 통제 기술, 새로운 바이러스·웜 탐지 기술, 익명인증, 소셜 네트워크 서비스를 이용한 개인정보 침해 및 불

건전 정보 유통을 방지할 기술 개발, 온오프라인 연계형 ID관리 기술 및 개인정보 보호 기술, 사이버윤리 및 범죄 제어 및 웹과 연계된 선행 보호기술과 능동적 대체 기술, 소셜네트워킹 기반의 사용자 신원확인 서비스가 필요하다.

4. 미래 인터넷 변화에 따른 역기능의 발생 예상시기와 피해강도

미래 인터넷 변화에 따른 역기능 및 문제점과 관련해서 전문가들은 2016년 이전에 다양한 현상이 발생할 가능성이 있다고 예상하고 있다 <표 5>. 역기능발생 예상시기가 가장 빠른 대상 (다양한 ID 사용증가, 2010.8년)과 가장 지연된 대상 (Seamless 인터넷환경 도래, 2015.6년)의 시간 차이는 약 4.8년으로 비교적 단기간 사이에 인터넷에서의 다양한 역기능이 예상된다고 할 수 있다. 이러한 전문가들의 의견은 개별 항목에 대한 구체적인 발생 시기 그 자체가 갖는 중요성 뿐 아니라 일반인들이 피부로 느끼고 있는 인터넷 환경의 급격한 변화와 그에 따른 취약성을 재확인하는 연구결과로서 의미를 갖는다.

<표 5> 미래인터넷 변화에 따른 역기능 항목별 예상발생시기

미래인터넷 변화상	역기능발생 예상시기
다양한 ID사용 증가	2010.8
개인정보 경제가치 증가	2011.3
웹기반 서비스 경제활성화	2012.7
기술발전 속도 차이	2012.9
정보소통과 통제	2013.0
인터넷에서 국가 경계변화	2013.1
인터넷 속도 증가	2013.2
미디어 데이터 증가	2013.2
클라우드 컴퓨팅	2013.4
Social Network의 발전	2013.5
대용량 데이터 집적	2013.7
Internet of Things	2015.5
Seamless 환경	2015.6

예상 시기를 구체적으로 살펴보면, 인터넷을 통해 다양한 서비스를 이용하는데 필요한 개인식별 번호나 기호 (ID: Identification) 사용이 증가함에 따라 발생 가능한 역기능 (2010.8년)과 개인 정보의 경제적 가치가 증가하면서 나타나는 문제점 (2011.3년)은 다른 항목들에 비교해서 상대적으로 빨리 발생할 것이라고 예상된다. 한편, 정보통신기술의 발달에 힘입어 물리적 공간의 사물에 내재한 네트워크를 통해서 사물 간 컴퓨팅과 커뮤니케이션이 확대(Internet of Things, Internet with Things)됨으로써 광범위하게 발생 가능한 문제점 (2015.5년)과 사물, 시스템에 내제된 센서 등의 통신장치를 통해 시간, 장소에 관계없이 데이터의 저장이나 사용이 끊김 없이 지속되는 서비스 환경(Seamless 환경)에서 나타나는 역기능 (2015.6년)은 상대적으로 지연되어 나타날 것이라고 예상된다.

미래 인터넷 환경 하에서 발생 가능한 역기능 및 문제점의 피해강도 (impact)는 대체로 높은 것으로 나타났다 <표 6>. 즉, 전체 설문항목 13개의 피해강도 총 평균은 4.18 (5점 척도: 1, 매우 낮다; 3, 보통; 5, 매우 높다)로 나타났다. 이 가운데 개인정보의 경제적 가치가 증가함에 따라 발생하는 역기능의 피해강도 (4.6점)와 정보통신기술의 발달에 힘입어 물리적 공간의 사물에 내재한 네트워크를 통해서 사물 간 컴퓨팅과 커뮤니케이션이 확대(Internet of Things, Internet with Things)됨으로써 발생하는 문제점의 피해강도 (1.5점)가 다른 항목에 비해서 상당히 높은 것으로 나타났다. 한편, 인터넷 관련 기술발전의 속도 차이에 따른 피해강도 (2.5)와 인터넷 속도 증가 (2.2)및 미디어 데이터 증가 (2.2)에서 비롯된 역기능의 피해강도는 어느 정도 높을 것으로 평가되지만 본 설문조사에 포함된 다른 항목에 비해서는 상대적으로 피해강도가 낮게 나타났다.

<표 6> 미래인터넷 변화에 따른 역기능 항목별 피해강도

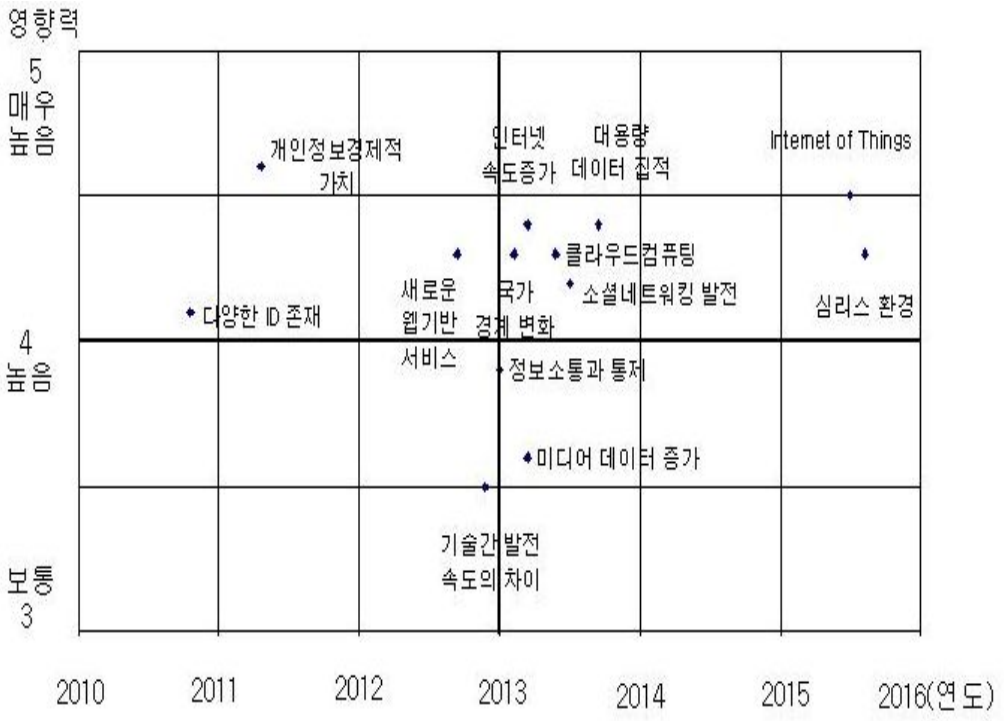
미래인터넷 변화상	역기능 피해강도
개인정보의 경제적 가치	4.6
Internet of Things	4.5
대용량 데이터의 집적	4.4
인터넷속도 증가	4.4

인터넷에서의 국가경계 변화	4.3
클라우드컴퓨팅	4.3
새로운 웹기반 서비스	4.3
심리스 환경	4.3
소셜 네트워킹의 발전	4.2
다양한 ID 존재	4.1
정보소통과 통제	3.9
미디어 데이터 증가	3.6
기술간 발전속도의 차이 발생	3.5

5. 미래 인터넷 변화에 따른 역기능의 유형화

미래 인터넷 변화에 따른 역기능 및 문제점이 발생할 예상시기와 그에 따른 피해 강도를 분석함으로써 13개 미래인터넷 변화상에 대한 역기능을 유형화 할 수 있다. <그림13>과 같이 가로축 (X축)은 역기능 발생 예상시기를 나타내며, 세로축 (Y축)은 역기능 발생에 의한 피해강도를 표현하는 좌표 평면에 본 설문조사에서 나타난 13개 항목을 표시하였다. 역기능 발생 예상시기는 2013년을 중심으로 발생이 상대적으로 빠른 역기능과 느린 역기능으로 구분하였다. 이 기준에 따르면, 다양한 ID사용 증가, 개인정보 경제가치 증가, 웹기반 서비스 경제 활성화, 기술발전 속도 차이, 정보소통과 통제와 관련된 역기능은 비교적 빨리 (2013년 이전) 역기능이 발생할 것이라고 예상된다. 이에 비해서 인터넷에서 국가 경계변화, 인터넷 속도 증가, 미디어 데이터 증가, 클라우드 컴퓨팅, Social Network의 발전, 대용량 데이터 집적, Internet of Things, Seamless 환경에 따른 문제점은 발생년도가 상대적으로 지연된 (2013년 이후) 대상으로 구분된다.

<그림 13> 역기능 발생시기와 피해강도



역기능 피해강도는 4점(높은 피해)을 기준으로 피해 수준이 매우 높은 경우와 상대적으로 덜 높은 경우로 분류하였다. 본 설문조사에 포함된 13개 항목 가운데, 정보소통과 통제, 미디어 데이터 증가, 기술발전 속도 차이 등 3개 변화상에 대한 역기능의 피해강도는 상대적으로 덜 높다고 평가되었으며, 이외의 9개 변화상에 대한 역기능의 피해강도는 매우 높게 나타났다.

이러한 분석 결과를 요약, 정리하여 개별 변화상에 대한 역기능의 특성을 발생 예상시기와 피해강도를 기준으로 유형화하면 아래의 표와 같다. 역기능 발현시기가 빠르고 피해강도가 높은 유형 (I사분면)은 다양한 ID사용 증가, 웹기반 서비스 경제활성화, 개인정보 경제가치 증가 등 3개 항목을 포함한다. 발현시기는 늦지만 피해강도는 높은 유형 (II사분면)으로 Social Network의 발전, 국가경계 변화, 클라우드 컴퓨팅, 대용량 데이터 집적, Seamless 환경, Internet of Things, 인터넷

속도 증가 등 7개항목이 나타났다. 한편 발현시기는 늦고 피해강도는 낮은 유형(III사분면)에는 미디어 데이터 증가가 있다. 그리고 발현시기는 빠른데 피해강도는 낮은 유형 (IV사분면)으로는 기술발전 속도 차이와 정보소통과 통제가 있다.

<표 7> 미래인터넷 정보보안의 유형화

역기능 피해강도	역기능 발현 예상시기 (빠름)	역기능 발현 예상시기 (늦음)
(높음)	**I사분면** 발현시기 빠름 / 피해강도 높음 ● 다양한 ID사용 증가 ● 웹기반 서비스 경제활성화 ● 개인정보 경제가치 증가	**II사분면** 발현시기 늦음 / 피해강도 높음 ● Social Network의 발전 ● 국가경계 변화 ● 클라우드 컴퓨팅 ● 대용량 데이터 집적 ● Seamless환경 ● Internet of Things ● 인터넷 속도 증가
(낮음)	**IV사분면** 발현시기 빠름 / 피해강도 낮음 ● 기술발전 속도 차이 ● 정보소통과 통제	**III사분면** 발현시기 늦음 / 피해강도 낮음 ● 미디어 데이터 증가

가. 미래 인터넷 역기능의 특성과 정책적 대응논리[12)]

미래 인터넷 역기능을 발생 예상시기와 피해강도에 따라 유형화하는 것은 역기능과 문제점을 대비하기 위한 관리적 시각을 넓히고 대응책을 다양화하기 위한

12) 정익재 (2007). 정보보안 취약성 분석과 정책적 대응논리. 한국정책학회보, 16권 2호, pp. 211-238.

하나의 정책설계과정이라고 할 수 있으며, 이런 과정을 통해서 정보보안을 위한 대책을 탐구할 수 있는 분석틀을 마련할 수 있다. 본 조사에서 논의된 역기능에 대한 유형별 대응방안은 Morone과 Woodhouse (1986)[13]이 제시한 5가지 위험관리 전략을 중심으로 정책적 의미를 정리한다.

1) 우선순위 설정전략 (set priorities)

우선순위 설정전략은 특정 시점에 어떤 대상을 먼저 관리해야 할 것인지에 대한 체계적인 차별화를 의미한다. 이는 시간과 자원이 제한된 현실에서 모든 위험, 즉 역기능과 문제점을 한꺼번에 관리할 수 없다는 현실에 비추어 지극히 자연스러운 대응논리이므로 '전략'이기에 앞서 정책 '상식'이라고 할 수 있다.

본 조사에서 제시된 4개의 역기능 집단 가운데 I사분면에 포함된 역기능은 발생 예상시기가 빠르고 피해강도도 상대적으로 높기 때문에 다른 역기능에 비해서 정책 우선순위가 앞서며 그만큼 정보보안을 위한 관리 노력이 집중되어야 할 대상이다. 한편, III사분면에 해당하는 역기능은 발생 예상시기가 상대적으로 늦을 뿐 아니라 피해강도도 낮기 때문에 다른 역기능에 피해 정책 관심이 낮고 자원을 분배하는데 우선순위가 낮을 수 있다. II사분면과 IV사분면에 해당하는 역기능은 발생 예상시기는 늦지만 피해강도가 높거나 반대로 발생 예상시기는 빠른데 피해강도가 낮으므로 정책 우선순위가 I사분면보다는 낮고 III사분면에 비해서는 높은 대상이라고 할 수 있다. 이들 두 유형에 대한 정책 논의, 즉 우선순위 설정은 정보보안과 시스템 역기능을 관리하는 조직이나 담당자의 시각과 대응능력에 따라 달라질 수 있다.

정보보안 문제 또는 역기능의 발생 예상시기가 언제인지에 대한 관심보다는 일단 문제가 발생하고 이에 따른 피해 규모와 강도에 중요성을 부여하거나 심각한 피해를 가져올 수 있는 최악의 상황을 상정하여 대응하려는 위험 회피적인 시각과 더불어 불확실한 상황을 대처하는데 비관적이고 소극적인 태도를 갖는다면, IV사분면보다는 II사분면의 역기능에 대해서 정책 자원이 집중 배분되어야 한다.

---

13) Morone, Joseph G & Woodhouse, Edward J. (1986). *Averting Catastrophe: Strategies for regulating risk technologies.* Berkeley: University of California Press.

특히, II사분면에 포함된 Internet of Things와 대용량 데이터 집적에 따른 역기능의 발생 예상시기는 상대적으로 늦지만 피해강도가 본 논문에서 분석된 역기능 가운데 상당히 높은 대상이라는 점에서 II 사분면에 대한 정책 우선순위가 높다고 볼수 있다. 한편, 피해 강도는 클지라도 발생 예상시기가 상대적으로 느린 역기능보다는 피해 강도가 작을지라도 발생 예상시기가 빠른 역기능에 대해서 관심이 집중되어야 한다는 시각, 즉 역기능으로 인해서 심각한 결과를 초래할 사고가 발생할 가능성은 높지 않지만 단 시일 내에 발생 가능한 역기능에 대해서는 대응능력이 어느 정도 축적되어 있다고 판단하는 낙관적이고 적극적인 시각에 따른다면 II사분면 보다는 IV사분면에 관심이 모아지고 그만큼 정책 자원도 우선 배분되어야 한다.

2) 잠재적인 위험방지 전략 (protect against the potential hazard)

잠재적인 위험방지 전략은 심각한 결과를 초래할 수 있는 위험을 관리·대응하는 것이 어렵거나 불가능한 경우, 최악의 상황을 방지하기 위한 전략으로 초기의 원자력 연구개발 분야에서 주로 적용되었다. 이 전략의 구체적인 형태로는 대규모 재난을 가져올 수 있는 기술이나 행위를 사전에 완전히 금지 (prohibition)시키는 방법, 위험을 유발할 수 있는 대상이나 요소를 봉쇄 (containment)하는 방법, 현실적으로 금지나 봉쇄가 어렵고 재난의 규모가 상대적으로 작을 경우는 사용을 제한 (limit to use)하거나 선별적으로 사용을 방지 (prevention)하는 방법, 위험발생의 가능성을 어느 정도 인정하고 일단 사고가 발생하면 대규모 재난으로 확대되는 것을 방지하고 완화 (mitigation)하는 방법이 있다.

잠재적인 위험방지 전략은 정보보안 문제나 역기능이 발생하였을 때 피해강도가 큰 대상에 적용하는 것이 적절하므로 I사분면과 II사분면에 포함된 역기능이 이에 해당한다. 특히 피해강도 뿐 아니라 발생 예상시기가 빠른 I사분면의 개인정보 경제가치 증가와 II사분면의 Internet of Things와 대용량 데이터 집적에 따른 역기능을 대상으로 적용할 수 있다. 하지만 잠재적인 위험방지 전략 가운데 가장 보수적인 수단이라고 할 수 있는 "금지"를 정보통신기술 또는 인터넷에 적용하기에는 한계가 있다. 고도 정보화 사회가 유발할 수 있는 문제점과 광범위한 네트워

크 활용으로 인해서 발생 가능한 극단적인 피해를 우려하여 정보통신 기술개발을 포기하거나 인터넷 사용을 금지하는 것은 현실적인 대안이라고 할 수 없기 때문이다. 비록 정보통신기술 그 자체를 금지하는 것은 아닐지라도 특정 운영시스템의 치명적인 결함과 그에 따른 피해를 최소화하기 위해서 "금지"라는 대응수단을 취할 수는 있다. 예를 들어 인터넷을 통해서 특정 시스템에 접근할 때 요구되는 인정절차를 만족시키지 못하면 시스템의 사용을 "금지"하는 것이 이에 해당한다.

"봉쇄"는 일상적인 시스템 운영을 전제로 취약점을 악용하려는 징후나 역기능의 사전 경고가 있을 경우 시스템을 정지·차단하는 조치를 의미하는데, 대체로 국가 안보, 국방, 또는 범죄와 같이 문제발생에 따른 사회적인 파급효과가 큰 분야의 시스템을 대상으로 적용할 수 있다. 금지와 봉쇄는 역기능으로부터 시스템을 보호하는데 효과적이지만 시스템을 정상적으로 사용할 수 없다는 불편함이 동시에 발생한다. 전자정부 포탈사이트와 같이 방문자와 사용자가 많은 시스템을 금지 또는 봉쇄할 경우 그 만큼 사회적 비용을 유발할 수 있다. 이런 경우 시스템의 접근과 사용을 제한하거나 선별적으로 허용하는 조치를 취할 수 있다. 예를 들어, 사용자가 시스템에 접근하는데 요구되는 패스워드나 암호를 입력하면서 일정 횟수의 오류가 발생하면 시스템을 한시적으로 차단하고 사용자의 신분이나 목적을 재확인함으로써 보안 사고에 줄일 수 있다. 시스템의 사용 제한이나 선별적 허용 조치는 보안사고 발생에 따른 사회적 피해강도가 안보, 국방, 치안과 같이 매우 심각하지는 않지만 정보보안을 위한 높은 수준의 주의이 요구되는 분야, 예를 들면, 의료, 금융, 교육 분야와 같이 개인자료의 오용과 더불어 사생활침해가 발생할 수 있는 대상에 적용 가능하다.

3) 위험검사 전략 (test the risks)

위험검사 전략은 일정한 통제나 제약조건 하에서 위험에 대한 실험을 실시하고, 보안사고의 진행과정과 피해내용 및 결과를 분석하여 유사한 상황이 발생할 경우 이를 활용하여 위험에 대응한다. 예를 들면, 정보보안과 관련해서 침투실험이나 모의 해킹을 실시하여 시스템의 역기능을 점검하거나 조직의 정보보안 대응능력을 분석하여 시스템의 완결성을 높이고 보안정책을 재조정하는데 실험 결과를

반영한다.[14] 위험검사 전략은 발생 예상시기가 빠르지 않아 침해 방법, 과정, 결과에 대한 사전경험, 지식, 그리고 대응능력이 상대적으로 누적되지 않은 역기능, 그리고 보안사고 발생으로 인한 피해강도가 사전 모의실험이 필요할 정도로 높은 역기능에 적용 가능하다. 즉, II사분면에 포함된 역기능이 사전검사 전략의 적용 대상으로 적절하다고 판단된다. 예를 들어 대용량 데이터 집적에 따른 역기능의 경우, 일상적으로 시스템을 활용하는 상황을 상정하여 이에 준하는 데이터의 할당 용량을 정하거나 허가 받지 않고 불법으로 시스템에 접근할 수 있는 침해기술의 현 수준을 고려하여 시스템을 통제하는 경우, 예외적인 수단이나 예측하지 못 했던 환경에서 시스템이 보안침해에 노출될 수 있다. 이러한 역기능은 시스템 설계자나 보안담당자의 기존의 지식 범위와 기술 수준을 벗어나는 전혀 생소하고 예기치 않았던 역기능일 가능성이 있으므로 다수의 보안침해전문가의 다양한 침투실험을 통해서 새로운 역기능과 침해기술을 발견하고, 이와 더불어 대응 방안과 기술을 마련할 수 있는 기회를 제공한다..

4) 신중한 진행전략(proceed cautiously)

정보보안 역기능으로 인한 피해 강도와 심각성을 사전에 파악한다는 것은 쉽지 않다. 그만큼 특정 보안사고나 역기능에 대한 대응조치가 어느 정도의 수준에서 정당화되어야 할 것인지에 대해서 논란의 여지가 있다. 돌이킬 수 없는 피해를 가져올 보안사고에 대해서는 앞에서 언급한 가장 보수적이라고 성격지울 수 있는 완전금지(prohibition)나 봉쇄(containment) 조치를 택할 수 있다. 하지만 많은 경우, 극단적인 대응조치를 취하기보다는 시스템이나 네트워크를 사용함으로써 유발

14) 행정자치부는 2005년 9월 안철수연구소에 전자정부 통합망으로 연계돼 있는 78개 국가기관 가운데 17곳에 대한 모의 해킹을 의뢰했다. 그 결과에 따르면, 13곳의 전산망이 해커에게 뚫린 것으로 밝혀졌다. 특히 국무총리 비서실, 공정거래위원회, 통계청, 민주평화통일자문회의 등 4곳은 '서버 관리 권한'까지 해킹당할 정도로 보안이 매우 취약한 것으로 나타났다. 환경부, 소방방재청, 충남도청은 '일부 관리 권한'을 해킹당해 '서버 관리 권한'까지 해킹당한 4곳과 함께 보안 수준이 '매우 취약하다'는 판정을 받았다. 서버 관리 권한이 해킹됐다는 것은 컴퓨터 서버에 저장돼 있는 모든 정보에 대한 복사, 삭제, 변경 등의 권한이 해커의 손에 넘어갔다는 뜻이다. 실제 상황이라면 국민의 사생활 정보는 물론 공정위의 기업 관련 조사 자료 등이 유출될 수 있다. 통계청이 지난해 실시한 인구주택총조사 항목에 포함된 혼인여부, 가장의 직장과 직위 등도 유출 또는 조작당할 위험성이 있다. (동아일보 2006년 8월 31일)

되는 사회적 편익과 보안침해에 따른 비용을 상대적으로 고려하여 보안규제와 대응조치의 수준을 결정해야 한다는 논리가 신중한 진행전략의 핵심 내용이다. 보안사고로 인하여 피해가 발생할 가능성이 있음에도 불구하고 시스템을 사용하는 것을 상정하는 신중한 전행전략은 혹시 보안사고가 실제로 발생할지라도 피해강도가 상대적으로 낮은 III사분면과 IV사분면의 역기능을 대상으로 적용가능하다. 하지만 피해강도가 낮을지라도 자주 발생하거나 조만간 발생할 역기능을 대상으로 "신중하게 진행한다"는 이유로 재발을 방치하는 것은 합리적인 보안관리라고 할 수 없다. 따라서 신중한 진행전략은 피해강도가 낮고 발생 예상시기가 늦은 III사분면에 해당하는 역기능에 보다 더 효과적으로 대응할 수 있다. 인터넷 속도 증가와 미디어 데이터 증가에 따른 역기능과 문제점은 초기에 발견하기 쉽지 않고 새로운 인터넷 환경이 현실화되고 어느 정도 시간 경과하면서 나타나는 경향이 있으므로 이와 관련된 역기능에 대해서는 보안사고에 대응할 최소한의 조직 역량과 자원을 갖춘 상황에서 시스템을 계속 사용하고, 혹시 보안사고가 발생하거나 새로운 역기능이 발견되면 그 파급효과를 줄이고 관련 지식과 경험을 축적할 수 있다.

5) 경험에 의한 학습전략 (learn from experience)

학습전략은 보안사고가 발생하는 것을 상정하고 사후적으로 진행되는 관리과정이라는 점에서 "신중한 진행전략"과 유사하다. 바람직하지는 않지만 보안사고나 역기능이 빈발하면 할수록 다양한 경험이 축적되고 효과적인 학습이 이루어질 수 있다는 점에서 피해 강도가 낮고 발생 예상시기가 빠른 IV사분면에 포함된 역기능에 적용할 수 있다. 이러한 경우 학습전략에 따라 시스템을 정상적으로 운영하면서 발생하는 새로운 역기능의 특성을 지속적으로 분석하고 이를 근거로 대응방안을 수립하는 것이 필요하다.

학습전략은 기존의 대응전략이나 보안기술 하에서 발생한 예기치 않았던 결과를 관찰함으로서 새로운 안전조치의 필요성을 결정하는 전략이므로 시행착오(trial and error)를 전제로 하고, 침해사고 발생에 의한 제한된 범위의 손실을 인정해야 한다. 비록 무오류시행 (trial without error)에 의존한 학습이 가능하다면 가장 바람직하겠지만 불확실성을 배경으로 발생하는 보안문제와 역기능은 오류나

실수로부터 자유로울 없다. 정보보안 문제와 시스템 역기능이 기술적인 원인 뿐 아니라 조직관리, 사회문화 및 심리적 요인에 의해서 발생한다면, 오류 없이 시스템을 개발하거나 관리한다는 것은 현실적으로 불가능하다. 결국 정보보안과 관련된 정책을 논하는데 무오류시행을 상정할 수는 없으며, 오류가 발생할 가능성이 있는 경우 시행을 하지 않는 전략, 즉 역기능이나 보안침해의 발생이 불가피하다면 원천적으로 시스템을 개발하지 않거나 사용하지 않는 것을 생각할 수 있다. 이는 결국 잠재적인 위험방지 전략의 하나인 '금지'에 해당하는 논리로서 현실적으로 수용하기 어려운 대응방안이다. 현실에서 정보보안 침해라는 위험을 두고 시행착오를 허용한다면 매우 무책임하고 비윤리적인 행동이라고 비난받을 수 있고 그만큼 사전 예방조치에 대한 선호가 높은 이유라 할 수 있다. 하지만 역기능의 발생원인, 배경, 경로, 그리고 피해 결과에 대해서 명확한 예측할 수 없는 경우 이에 대한 어떠한 사전적 조치와 대응책은 오히려 자원 낭비와 더불어 예기치 않았던 결과에 대한 신속하고 유연한 대응을 방해함으로써 더 큰 피해를 가져올 수 있다. 즉, 누구도 예견하지 못한 의외의 사태 바로 그 자체가 더 큰 위험이고 사고라는 점을 인식하는 것이 쉽지 않다. 따라서 피해강도가 상대적으로 낮은 역기능에 대해서 학습전략의 적용 가능성에 관심이 집중된다.

나. 역기능 유형화의 정책적 함의

본 연구에서 이루어진 미래 인터넷 환경에서 역기능의 유형화와 개별 유형의 특성에 따르면, 정보보안을 위한 정책 노력과 관심이 어디에 우선 집중되어야 하며, 특정 역기능 유형에 대해서 어떤 대응 전략이 보다 효과적인가에 대한 정책 방향을 도출할 수 있다. 발생 예상시기가 빠르고 피해강도가 모두 높은 역기능에 대해서는 잠재적 위험방지 전략, 발생 예상시기는 늦은데 피해강도가 높은 역기능은 위험검사 전략, 발생 예상시기가 늦고 피해강도가 낮은 역기능은 신중한 진행 전략, 그리고 발생 예상시기는 빠른데 피해강도는 낮은 역기능은 학습전략을 적용하는 것이 적절하다고 판단된다. 물론 이러한 분석 결과가 특정한 역기능에 대해서 하나의 전략으로 보안침해를 완벽하게 해결할 수 있다는 것을 의미하지는 않는다. 역기능의 발생 예상시기와 피해강도라는 주요 요인을 고려하여 역기능을 집

단별로 특성화, 차별화함으로서 보안문제를 보다 체계적으로 관리하는데 활용할 수 있는 정책 지침으로서 중요성을 갖는다.

역기능을 관리하기 위해서 논의된 다양한 전략은 보안침해 문제가 발생하기 이전에 미리 대비하거나 차단하는 예방 (anticipation) 전략과 침해 사고가 발생한 다음 사후적으로 피해를 최소화하거나 사고를 관리하는 과정에서 노정된 문제점을 보완하는 복원 (resilience) 전략으로 대별할 수 있다. 잠재적인 위험방지 전략에서 논의된 금지, 봉쇄, 사용제한 등과 같은 조치들은 전자에 해당한다. 한편 위험검사 전략, 신중한 진행전략, 그리고 학습전략은 후자에 포함되는 구체적인 사례라고 할 수 있다. 특히, 복원전략에 해당하는 전략들은 각각 독특한 내용과 유용성을 갖고 있으며, 정도의 차이는 있지만 학습을 강조하고 있다는 공통점을 갖는다. 즉, 위험검사전략은 인위적, 의도적으로 시스템의 취약점이나 역기능을 찾고자 시도하고, 신중한 진행전략은 침해사고가 발생할 가능성이 있음에도 불구하고 통제가능한 범위 안에서 시스템을 정상 운행하고 사고가 실제 발생하면 자료를 수집 분석하여 보안체계를 개선하는데 초점을 둔다는 점에서 결국 정보보안 사고를 관리할 수 있는 조직의 역량을 학습과정을 통해서 높이고자 노력한다.

학습과정은 자연스럽게 이루어지는 것이 아니라 이를 체계적으로 관리, 촉진할 수 있는 제도적 기반이 마련되어 있어야 한다. 예를 들면, 새로운 역기능의 발생원인과 빈도, 파급과정 및 효과, 그리고 대응과정 등에 대한 데이터를 수집, 분석, 관리하는 것은 기본이며, 이러한 과정을 통해서 습득된 내용은 학습대상 집단이나 개인에게 효과적인 방법을 통해 전달되어야 한다. 또한 학습은 일회성 행사가 아닌 체계적이고 지속적인 지식공유 과정이므로 학습이 이루어진 다음 이를 평가하여 미흡한 점을 보완하는 활동도 포함된다. 즉, 학습과정의 제도화는 정보보안과 관련해서 위험관리시스템의 구축을 의미하며, 정보보안 활동은 위험관리시스템 하에서 시행착오를 통한 점진적인 변화를 추구하는 문제풀이 과정이라고 할 수 있다. "정보보안은 기술이 아닌 위험에 관한 것이며, 위험을 관리하는 또 다른 방법이다. 정보보안은 결과가 아닌 과정을 의미한다."[15]는 보안전문가 Schneier (2003:

15) Security is not about technology. It's about risks, and different ways to manage those risks. It's not a product; it's a process (Schneier, 2003: 146)

146)의 주장은 본 연구가 담고 있는 정책적 시사점을 함축하여 전달하고 있다.

인간이 만든 어떤 기술도 취약점과 역기능으로부터 자유로울 수 없음에도 불구하고, 기술의 진보와 발전은 안전성보다 능률성에 의해서 정당화되어 사회적으로 수용된다. 정보통신 기술을 활용함으로써 경험하고 있는 현실의 편리함과 실현 가능한 미래의 화려함은 안전성에 대한 무관심을 유발하기에 충분하다. 산업사회에서 노정되었던 안전에 대한 무지, 편견, 외면은 정보사회에서 그대로 전이되어 나타나고 있는 현실에 대한 관심과 우려에서 출발한 본 연구는 정보보안의 문제와 대응방안을 기술공학적 시각이 아닌 정책적 논리를 통해서 접근하였다. 특정한 역기능이나 보안침해 사고에 대해서 구체적인 해결책을 제시할 의도에서 시작한 연구가 아니기에 본 연구의 분석결과와 정책 제언을 현실에 직접 적용하는데 어려움이 많을 수 있다.

제5장 미래인터넷 환경에서의 정보보호 방안

제1절 정책적 우선순위

앞서 조사한 전문가 대상 설문결과는 미래인터넷 환경의 변화에 따라 나타나는 역기능의 영향력 강도와 발현시기를 조사함으로써 이에 대한 우선순위를 전망해 볼 수 있다. 미래인터넷 환경에서의 개별 역기능의 특성을 발생 예상시기와 피해강도를 기준으로 유형화하여 우선순위에 따라 정책적 우선순위를 정할 수 있다.

첫째, 역기능의 발현시기가 빠르고 피해강도가 높은 유형으로 우선적으로 대응이 필요한 부분이다. 다양한 ID사용 증가, 웹기반 서비스 경제활성화, 개인정보 경제가치 증가 등 3개 항목이 포함되어 있다. 사이버 위협순위도 개인정보유출이 1순위로 나타나듯 우선적으로 대응해야 할 과제도 개인정보유출이 우려되는 내용이 중심이 되고 있다.

역기능은 발생 예상시기가 빠르고 피해강도도 상대적으로 높기 때문에 다른 역기능에 비해서 정책 우선순위가 앞서며 그만큼 정보보안을 위한 관리 노력이 집중되어야 할 대상이다.

둘째, 다음순위가 될 수 있는 역기능의 발현시기는 늦지만 피해강도는 높은 유형으로 Social Network의 발전, 국가경계 변화, 클라우드 컴퓨팅, 대용량 데이터 집적, Seamless 환경, Internet of Things, 인터넷 속도의 증가 등 7개항목이 나타났다.

그리고 발현시기는 늦고 피해강도는 낮은 유형에는 미디어 데이터 증가가 있다.

이들 두 유형에 대한 정책 논의, 즉 우선순위 설정은 정보보안과 시스템 역기능을 관리하는 조직이나 담당자의 시각과 대응능력에 따라 달라질 수 있다.

정보보안 문제 또는 역기능의 발생 예상시기가 언제인지에 대한 관심보다는 일단 문제가 발생하고 이에 따른 피해 규모와 강도에 중요성을 부여하거나 심각한 피해를 가져올 수 있는 최악의 상황을 상정하여 대응하려는 위험 회피적인 시각과 더불어 불확실한 상황을 대처하는데 비관적이고 소극적인 태도를 갖는다면, 발현시기가 빠르고 피해가 낮은 유형 보다는 발현시기가 늦고 피해가 높은 유형

의 역기능에 대해서 정책 자원이 집중 배분되어야 한다. 특히, 발현시기가 늦고 피해가 높은 유형에 포함된 Internet of Things와 대용량 데이터 집적에 따른 역기능의 발생 예상시기는 상대적으로 늦지만 피해강도가 본 논문에서 분석된 역기능 가운데 상당히 높은 대상이라는 점에서 발현시기가 늦고 피해가 높은 유형에 대한 정책 우선순위가 높다고 볼 수 있다. 한편, 피해 강도는 클지라도 발생 예상시기가 상대적으로 느린 역기능 보다는 피해 강도가 작을지라도 발생 예상시기가 빠른 역기능에 대해서 관심이 집중되어야 한다는 시각, 즉 역기능으로 인해서 심각한 결과를 초래할 사고가 발생할 가능성은 높지 않지만 단 시일 내에 발생 가능한 역기능에 대해서는 대응능력이 어느 정도 축적되어 있다고 판단하는 낙관적이고 적극적인 시각에 따른다면 발현시기가 늦고 피해가 높은 유형 보다는 발현시기가 빠르고 피해가 낮은 유형에 관심이 모아지고 그만큼 정책 자원도 우선 배분되어야 한다.

셋째, 마지막 단계로는 발현시기는 빠른데 피해강도는 낮은 유형으로 기술발전 속도 차이와 정보소통과 통제가 있다. 이는 발생 예상시기가 상대적으로 늦을 뿐 아니라 피해강도도 낮기 때문에 다른 역기능에 피해 정책 관심이 낮고 자원을 분배하는데 우선순위가 낮을 수 있다.

제2절 미래인터넷의 정보보호 방안

미래인터넷 환경에서 보안이 필요한 환경변화에 대한 우선 순위는 앞절에서 살펴본바와 같이 다양한 ID사용 증가, 웹기반 서비스 경제활성화, 개인정보 경제가치 증가 등이 우선적으로 해결되어야 할 과제로 나타나고 있으며 개인정보 유출을 우려하는 바가 크다. 다음으로 소셜네트워크의 활성화, Internet of Things, 심리스 환경, 클라우드서비스 등에 의한 위협이 해결되어야 한다고 하여 사회공학적 해킹 대응이나 새로운 서비스에서의 정보보호 방안을 강구하고 기존의 악성코드 예방 및 대응, 웹공격 대응 등이 필요하다.

또한 미래인터넷에서는 설계 당시부터 보안성을 고려해야 하기 때문에 각각의 위협에 대한 주요대응방안을 알아보는 것이 중요하다.[16] 앞서 살펴 보았던 사이버

위협을 토대로 악성코드의 예방 및 대응, 해킹 등 사이버 공격으로 부터의 미래인터넷 시스템의 보호, 개인정보보호 강화, 주요기반의 보호, 증가, 개인정보의 유출, 사회공학적 해킹에 대한 대응, 새로운 환경에서의 보안으로 대응방안을 알아보도록 하겠다.

가. 악성코드의 예방 및 대응

먼저 악성소프트웨어와 사기에 대한 대응방안이다. 이와 관련된 대부분의 위협은 엔드 호스트의 낮은 보안성과 사용자의 잘 속는 경향에 기인한다. 하지만 어떤 공격은 인터넷 기반 구조와 프로토콜의 낮은 보안성을 철저히 이용한다. 따라서 미래인터넷을 설계할 때 위협을 경감시키는 방향으로 설계하는 것이 중요하다.

먼저 네트워크 기반 구조의 보안성에 기반한 위협의 대응방안에 대해 살펴보겠다. 이러한 대응방안으로 현재도 많은 기술들이 개발되었다. 예를 들면 BGP 에 보안기능을 강화한 sBGP 가 있다. 이는 잘못된 라우팅 정보 주입을 막고 패킷 스푸핑을 필터링할 수 있는 기능이 있다. 하지만 이 방법은 몇 개의 문제만을 푼 애드온 패치에 지나지 않는다는 것이다. 게다가 기존의 BGP를 sBGP로 업그레이드하는 데 드는 높은 비용 때문에 대부분의 기반구조에 적용되지 않고 있어서 있으나마나한 대응책일 뿐이다. 높은 레벨의 프로토콜은 튼튼하고 안전한 기반 구조를 바탕으로 구성되어 있어야 한다. 그러므로 미래인터넷의 구조는 책임성(Accountability)을 제공할 수 있어야 한다. Accountability 는 인증된 소스로부터 패킷이 추적될 수 있는 형태로 전송되는 것을 의미한다. 이것은 익명성과 불추적성에 기인한 현재인터넷의 구조적인 문제를 해결할 수 있는 중요한 요소이다.

DNS 와 Fast-Flux 에 대한 주요대응방안은 다음과 같다. 인터넷은 호스트가 안전하게 리모트 리소스를 이용할 수 있도록 룩업 서비스를 필요로 한다. 하지만 현재의 DNS 는 위와 같은 서비스를 제공하지 못한다. 따라서 미래인터넷은 부적절한 매핑의 삽입에 대응할 수 있는 강인하고 안전한 룩업 서비스를 제공해야한다. 이로 인해 Fast-Flux 네트워크와 캐시 포이즈닝 공격에 대응할 수 있을 것이다.

---

16) 서승우, 미래인터넷에서의 사이버 보안, 2009. 8.

미래에는 봇넷은 다른 형태의 커맨드 앤 컨트롤 (C&C) 기반 구조를 이용하여 더욱더 효율적이고 찾기 힘들어 질 것이다. 예를 들어 미래인터넷의 봇넷은 소셜 네트워크를 이용할 가능성도 있을 것이다. 따라서 미래 통신 프로토콜의 설계자는 프로토콜이 스팸이나 봇넷의 컨트롤 채널에 이용될 가능성을 미리 염두해 두어야 할 것이다. 따라서 이러한 오용을 막기 위한 메커니즘이 필요하고 또한 네트워크를 남용하는 사용자를 찾고, 막고, 제거하는 Accountability 를 추가하여야 할 것이다.

나. 해킹 등 사이버 공격으로부터 중요 기반 시스템의 보호

중요 기반 시스템의 가장 중요한 이슈 중의 하나는 기반 구조간의 상호의존성이다. 따라서 인터넷과 연결된 기반 구조는 통신 기반구조의 상호의존성에 의해 취약점을 가지게 된다. 가장 먼저 통신의 강인성과 가용성을 개선시키는 것이 필요하다. 현존하는 기술 중에 Eight Ingredients Framework of Communications Infrastructure 라는 기술이 있다. 이를 통해 미래 네트워크의 통신 구조의 취약점을 8개의 성분으로 나누어 각각 체계적으로 살펴볼 수 있다. 이러한 취약점 분석을 통해 전문가들은 취약점을 없애거나 경감시킬 수 있을 것이다. 이러한 위협 분석은 위협에 대해 정확한 정보가 없을 때는 비효율적이긴 하지만 위협이 어떠한 것인지 알게 되면 상당히 좋은 대응방안이 될 수 있다.

미래에는 중요 어플리케이션과 중요 기반구조에 인터넷을 사용할 수밖에 없다. 따라서 다음과 같은 대응방안을 생각해 볼 수 있다. 먼저, 매우 중요한 시스템과 인터넷은 완전히 분리시킨다. 다음으로 다른 중요 분야에 인터넷 도입을 철저히 제어한다. 이 두 가지 원칙으로 완벽히 위협을 막을 수는 없겠지만 하나의 가이드라인이 될 수는 있을 것이다.

또한 웹의 이용은 인터넷 사용자와 직접적으로 연결되는 부분으로 웹은 서비스를 위해서 모든 불특정 다수의 접근을 허용하고 있고, 사용자의 정보가 보관되어 있는 데이터베이스(DB)와 직접 혹은 간접적으로 연결되어 있다. 전통적인 방어 솔루션인 방화벽, 침입탐지시스템(IDS), 침입방지시스템(IPS)은 가용성이 최우선인 웹서비스를 위해서 웹 서비스에 대한 탐지하고 있거나 일부만 탐지하고 있어, 웹

공격에 효과적으로 대응할 수 없다. 공격자들은 방화벽 등의 보안솔루션으로 차단되어 있어 침투하기 어려운 시스템 자체를 공격하는것 보다는 개방되어 있는 웹에 대한 취약점에 대해 공격을 시도하게 되었고, 과거 보안을 고려하지 않고 개발되어진 웹사이트들이 공격 대상이 되고 있으며, 현재 운영되고 있는 웹사이트의 상당수가 취약한 것으로 확인되어 이에 대한 대응이 필요하다.

다. 개인정보보호의 강화

향후 미래인터넷에서 전개될 물리 공간과 디지털 공간에서는 수집된 대량의 데이터가 개인정보를 보호하고 자기정보통제권을 보장하는데 이용되어야 한다. 또한 개인정보는 필요한 조직들에게만 서비스 제공을 목적으로 공유되어야 하며, 개인정보보호기술(Privacy-enhancing Technology) 연구를 통해 데이터 보호 기능과 서비스가 설계단계에서부터 내장하도록 개선되어야 할 것이다.

그리고 규제체제의 개선을 통해 개인정보보호에 대한 사용자들의 요구와 빠르게 성장하고 급속도로 팽창하는 비즈니스의 혁신 사이에서 세심한 균형이 필요하며, 모든 참여자들 사이에 신뢰를 구축하고 수익을 공정하게 배분하며 네트워크화된 시스템 안에서 자신들의 데이터 소유권을 통제할 수 있도록 되어야 할 것이다. 이를 위해서는 기존 개인정보보호와 보안에 관한 법률을 미래인터넷에 맞게 수정하고 필요한 경우 새로운 법률을 제정하고 효과적으로 집행하여야 한다.

개인정보보호를 위한 기술로는 대용량 데이터 암호 기술, 익명성 보장 기술, 개인정보영향평가 기법 개발 및 가치산정기법 개발, 데이터 암호화, 사용자 인증, 접근제어, 암호화, 온라인 행동(타켓)마케팅 보안 기술, 개인정보 자기 통제권을 제공하기 위한 기술 개발이 요구된다. 또한 개인정보보호 기술-Usage Control 및 사용자 중심의 개인정보 프로파일링/이용기술, 법 제도 정책을 시스템 측면에서 인지하고 제어 가능한 정책 관련 기술, 개인정보의 오남용을 방지하기 위한 인증서비스, 저장매체, 안전삭제 시스템 등 개인정보 침해여부 실시간 확인 기술, 법적 처벌 강화, 전자서명 개인정보에 대한 사용료 지급 근거가 되는 접근기록/보존 등이 필요하다.

라. 사회공학적 해킹에 대한 대응

미래인터넷 환경에서 우려되는 사이버 위협중 사회공학적 해킹에 대한 위협은 인간의 심리를 악용하는 형태로 이에 대한 적절한 대응으로는 철저한 보안의식을 수립하는 것이 가장 핵심적인 요소라고 할 수 있다. 각 기업이나 단체들이 사회공학적 해킹에 대비한 교육에 사용할 수 있도록 정부차원에서 가이드라인을 마련하여 배포하고 정기적인 교육과 모의훈련을 실시할 필요가 있다.

또한 시스템 차원의 대비책을 적절히 병행하여 사용자의 수를 최소화하는 체계를 구축할 필요가 있다. 교육훈련에 대한 보완 통제 방안으로 사용자의 부주의를 예방할 수 있는 시스템의 기술 개발을 병행하고 주요정보에 대한 모니터링 시스템을 구축하여야 할 것이다. 즉 적법한 보안단계를 거치지 않고는 외부유출이 불가능 하도록 시스템을 구축하여야 한다. 인터넷을 이용함에 있어 그 보안 수준을 상시적으로 파악할 수 있도록하는 예방적 차원의 보안수준 점검 시스템도 필요하다.

아울러 이러한 사회공학적 해킹에 대해서 신속하게 대처할 수 있는 정부차원의 시스템을 구축하고 지속적인 연구개발이 필요하다. 정보기기의 종류와 활용범위의 증가, 새로운 IT서비스의 증가로 인해 발생할 수 있는 사회공학적 공격 통로를 예측하고 사용자에게 미리 위험성을 경고하여야 한다. 유포되고 있는 사회공학적 해킹의 현황을 신속하게 보도하여 피해 확산을 방지할 수 있는 시스템도 마련되어야 할 것이다. 개인정보의 수집이 용이해 지고 사회공학적 공격법이 정밀해짐에 따라 사용자가 사회공학적 해킹을 판별해 내는 것이 어려워지므로 이러한 시스템을 통해 공격유형 정보를 신속히 제공하여 확산을 방지하여야 할 것이다.

마. 새로운 인터넷 환경에서의 보안

최근 클라우드 컴퓨팅(Cloud Computing) 기술이 각광을 받으면서 해당 기술을 네트워크 서비스에 접목시킨 'CCN'(Cloud Computing Network) 기술이 주목 받고 있다. 높은 성능과 비용절감 효과를 통해 차세대 CDN(Contents Delivery

Network)서비스로 각광을 받으면서 시장에서의 입지를 강화하고 있으나, 적용분야 와 사용자층이 넓어지면서 보안부분에도 관심이 높아지고 있다.

또한 스마트 환경 및 모바일 환경에서의 보안 위협을 줄이는 방안을 강구하여야 한다. 스마트폰과 같은 모바일기기는 공격자들의 관심을 끌기에 충분한 매력이 있다. 이에 반해 파워 한계와 적대적인 환경에의 물리적 노출로 인해 모바일 기기는 본질적으로 전통적인 컴퓨터에 비해 방어하기 힘들 수밖에 없다. 미래인터넷에서 모바일 기기는 중요한 데이터를 많기 담고 있기 때문에 방어책을 찾는 것이 시급하다. 현재 존재하는 안티 바이러스 소프트웨어나 네트워크 스캐닝을 단순히 모바일 기기에 포팅하는 것으로는 부족할 것이기에 새로운 형태의 대응책을 찾아야 할 것이다.

또한 센서로부터 잘못 읽어 들인 데이터에 관한 대응책은 앞서 살펴본 것과 같은 Accountability 로부터 찾아봐야 한다. 데이터의 출처를 제공하거나 데이터의 소스, 데이터의 변경을 추적할 수 있어야 한다. 이것이 모든 오용을 막을 수 있는 것은 아니지만 최소한의 대응책은 될 것이다.

제6장 결 론

현재 인터넷의 한 부분인 초기 네트워크 프로토콜은 보안보다 성능에 초점이 맞춰져 있으며, 이에 따라 네트워크 보안 및 사용자 책임성을 강화하는데 필요한 "ID", "시간", 그리고 "위치" 등의 기본 개념이 결여되어 있다. 또한 현재 인터넷의 특징으로는 사용자의 행동에 반응하는 수동적 미래인터넷의 보안 정책이 여러 국가와 관리 도메인, 다른 법규를 준수하거나 고유의 보안 정책을 갖고 있는 다양한 관계자들과 관련된 인프라, 복합 애플리케이션 보호에 적합해야 한다는 점이다.

현재 인터넷의 보안 특징은 인터넷 보안이 사용자의 행동에 반응하는 수동적 형태이고 장비별 개별적인 보안 시스템이 적용되고 있으며, 문제가 발생된 후에나 감지가 된다는 점에 있다. 또한 보안 시스템은 기존의 시스템에 추가된 형태로 구현되고 네트워크에서 분리된 형태로 존재한다는 점 등이 있으며 미래 인터넷으로의 진화에 따라 이러한 특징들도 변화해야 한다. 미래 인터넷에서의 보안 특징은 보안 시스템이 스스로 판단하고 행동하는 능동적 형태를 가지며, 다중계층 통합 보안 시스템 적용이 필요하다는 점이다. 또한 프로세스의 실행과 동시에 항상 문제 발생 감지해야 하며, 기존의 시스템과 보안 시스템이 결합된 형태를 가지고 네트워크에 통합된 보안 시스템의 형태 이어야 한다는 점 등의 특징을 가진다. 미래 인터넷에서 보안은 시스템에 통합된 형태가 되므로 반드시 필요한 요소이다.

이를 위해서 본 보고서에서는 각국의 미래인터넷 연구 동향을 살펴보고 전문가 설문조사를 통해 사이버 위협과 정책우선순위를 도출하고 그 대응방안을 살펴보았다.

정책적 우선순위는 다양한 ID사용 증가, 웹기반 서비스 경제활성화, 개인정보 경제가치 증가 등의 환경변화에서의 정보보호가 우선시 되고 이외에 Social Network의 발전, 국가경계 변화, 클라우드 컴퓨팅, 대용량 데이터 집적, Seamless 환경, Internet of Things, 인터넷의 속도증가 등의 환경에 대한 정보보호도 서둘러야 할 것으로 나타나고 있다.

이에 대한 대응 방안으로는 사이버 위협별로 악성코드의 예방 및 대응, 해킹 등 사이버 공격으로 부터의 미래인터넷 시스템의 보호, 개인정보보호 강화, 주요기

반의 보호, 증가, 개인정보의 유출, 사회공학적 해킹에 대한 대응, 새로운 환경에서의 보안으로 대응방안을 제시하고 있다.

미래인터넷은 향후 인터넷의 발전에도 의미가 있겠지만 더욱더 중요한 것은 우리의 생활 자체가 인터넷화한다는 점에서 인터넷의 발전을 바라봐야 한다는 점이다. 미국 등 선진국에서는 현재 인터넷의 문제를 극복하고 다음세대의 인터넷의 구축에 만전을 기하고 있으나 우리나라에서는 아직도 연구의 초기 단계로 미래인터넷에 대한 연구가 활성화 되어야 할 것이다.

더욱이 정보보호에 대한 연구는 국외에서도 사례를 찾아보기 어려우며 국내에서도 아직은 관련 연구가 부족한 실정이다. 차후 안정적인 인터넷 환경을 구축하기 위해서는 정보보호가 반드시 고려되어야하며, 정보보호 대책을 수립하기 위한 본격적인 연구가 필요하다 하겠다. 본 연구는 미래인터넷 환경에서의 정보보호문제와 대책을 살펴보기 위한 서설적인 연구로 향후 개인정보보호대책 등 분야별 대책수립이 필요하다. 본 연구는 이러한 연구나 정보보호 대책의 수립을 위해 기초가 될 수 있을 것이다.

<참고문헌>

□ 국내 문헌

o 논문 및 단행본

KISA, EU의 미래인터넷 동향 분석, CSO 브리핑, 2009. 7.

TTA 표준화 로드맵 2009 - 미래인터넷

김대영, 미래네트워크, TTA 저널, No112, 2007.

김방룡 외, EU의 미래 ICT 전략 동향, ETRI, 전자통신동향분석 제24권 2호, 2009. 4.

백은경, 미래 네트워크 기술 동향, IITA, 주간기술동향 통권 1387호, 2008.3.

신명기, 미래인터넷 기술 및 표준화 동향, ETRI 전자통신동향분석, 2007. 12.

신명기, 김은숙, 백은경, 황진경, New Study Item on Future Network Architecture and Services, in Proc. ITU-T Meeting, Seoul, Jan. 2008

정보통신연구진흥원, 유럽의 i2010 계획의 성과와 향후 추진 방향, 주간기술동향, 1359호, 2008. 8. 13.

정익재, 정보보안 취약성 분석과 정책적 대응논리. 한국정책학회보, 2007. 16권 2호

□ 국외 문헌

Amazon, 'Amazon Elastic Compute Cloud (Amazon EC2)',http://aws.amazon.com/ec2

Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, And Nei Kato, Abbas Jamalipour, "A survey of routing attacks in mobile ad hoc networks", IEEE Wireless Communications, October 2007

Delaney, D.; Ward, T. & McLoone, S. (2006), 'On Consistency and Network Latency in Distributed Interactive Applications: A Survey - Part I',

Presence: Teleoperators & Virtual Environments 15(2), 218-234.

Delaney, D.; Ward, T. & McLoone, S. (2006), 'On Consistency and Network Latency in Distributed Interactive Applications: A Survey - Part II', Presence: Teleoperators & Virtual Environments 15(4), 465-482.

European Commission, A Public-Private Partnership (PPP) for the Future Internet, 2009. 4.

European Commission, Future Internet 2020, 2009. 5.

European Commission, The Future of the Internet, 2009.

F.B. Schneider. Enforceable security policies. J. of the ACM, 3(1):30 - 50, 2000.

FIF: Future Internet Forum. http://fif.kr/

FIND: Future Internet Design. http://www.nets-find.net

Future Internet Portal. http://www.future-internet.eu/

Future Internet Socio-Economics (FISE) Working Group. http://www.smoothit.org/wiki/pmwiki.php/FISE

G. Karjoth, B. Pfitzmann, M. Schunter, and M. Waidner. Service-oriented assurance comprehensive security by explicit assurances. In Proc. of QoP-05. Springer, 2004.

G. Tselentis et al., Towards the Future Internet, IOS Press, 2009.

GENI: Global Environment for Network Innovations. http://www.geni.net/

Hinchcliffe, D. (2008), 'The Next Evolution in Web Apps: Platform-as-a-Service(PaaS)', Technical report, Hinchcliffe Company, http://bungee-media.s3.amazonaws.com/whitepapers/hinchcliffe/hinchcliffe0408.pdf

K. Papadopoulos, S. Voliotis, A. Ktena, P. Trakadas, Th. Zahariadis, "Security Aspects in Wireless Sensor Networks," Int. Conference on Telecommunications and Multimedia (TEMU 2008), Ierapetra, Crete, Greece, 16-18 July 2008

N. Dragoni, F. Massacci, K. Naliuka, and I. Siahaan. Security-by-contract:

Toward a semantics for digital signatures on mobil code. 2007.

N. Feamster, L. Gao, J. Rexford; How to lease the Internet in your spare time; ACM SIGCOMM Computer Communications Review, Vol. 37, No.1, January 2007

P. Trakadas, T. Zahariadis,H.C. Leligou,S. Voliotis, K. Papadopoulos, "AWISSENET: Setting up a Secure Wireless Sensor Network,"50th International Symposium ELMAR-2008, focused on Mobile Multimedia, Zadar, Croatia, 10-13 September 2008.

S3MS. Security of software and services for mobile systems. http://www.s3ms.org/, 2007.

Sachiko Yoshihama, Takeo Yoshizawa, Yuji Watanabe, Michiharu Kudoh, and Kazuko Oyanagi. Dynamic information flow control architecture for web applications. In Computer Security - ESORICS, pages 267-282, 2007.

V. C. Giruka, M. Singhal, J. Royalty, S. Varanasi, "Security in wireless sensor networks", Wirel. Communications Mob. Comput. 2008; 8:1-24.

Y. Karabulut, F. Kerschbaum, F. Massacci, P. Robinson, and A. Yautsiukhin. Security and trust in it business outsourcing: a manifesto. In Proc. of STM-06, volume 179, pages 47-58. ENTCS, 2007.

일본 정보통신연구기구, 신세대 네트워크 기술전략, 2009. 3.

[부록1] 전문가 대상 델파이 설문지

미래인터넷 환경에서의 선제적 보안대책 연구

본 설문서는 방송통신위원회 정책연구과제인 「미래인터넷 환경에서의 선제적 보안정책연구」를 수행하는데 필요한 자료를 수집하기 위하여 작성되었습니다. 정보통신환경이 변화하면서 미래사회에서의 인터넷 발전 전망과 그에 따른 사이버 위협과 대응방안을 모색하기 위한 연구과제입니다.

현재의 인터넷 이용환경을 개선하고 주도권을 확보하기 위해 각국에서 노력하고 있습니다. 그러나 향후 미래인터넷의 활성화를 위해서는 정보보호가 전제되어야 하며, 이를 위한 전략적인 대응이 필요합니다. 이에 미래사회에서의 인터넷과 사이버위협과 그에 대한 대응방안을 모색해 보고자 합니다.

선생님께서 응답하신 내용은 조사분석 이외의 목적으로는 사용되지 않습니다. 바쁘신 가운데 설문서 작성을 부탁드려서 죄송스럽게 생각합니다. 설문서에 나타난 선생님의 고견이 저희 연구에 중요한 자료로 활용된다는 점을 감안하시어 귀중한 시간을 할애하여 주시면 감사하겠습니다.

2009년 8월

< 설문 응답 요령 >

① 해당란에 √ 또는 o 로 체크

② 직접 기술해야 하는 대응방안은 자유롭게 기술

- 가능한한 구체적으로 기술 요망

③ 기타란 및 추가의견은 자유롭게 기술

<설명: 미래인터넷의 변화상>

● 미래인터넷환경의 변화상은 최근 EU에서 발표한 「미래인터넷 2020(Future Internet 2020)」의 변화상을 토대로 함

※ 미래인터넷 2020은 미래생활상을 구체적으로 묘사한 시나리오를 구성, 실제 미래상을 그려봄으로써 미래인터넷의 성공적 실현을 위해 준비해야 할 부분들을 보다 다차원적으로 탐구하고 포괄적으로 분석·검토

구분 / 변화상	해당 서비스의 활성화 시기는? (현재 ~ '20년)	사이버위협 및 역기능 등 문제점 발생 시기는?	가능한 사이버 공격유형 및 역기능은?	사이버위협 및 정보보안 사고가 미치는 임팩트 정도는?	사이버위협에 대한 대응방안(우선적으로 고려해야할 사항 표시 후 관련내용 기재 요망)	정보보호를 위해 꼭 필요한 핵심기술은?	핵심정보보호 기술의 可用연도는?
o 인터넷 속도 증가 인터넷 속도가 증가('20년에 유선 10G, 무선 1G로 증가예상)	◎ 2009 ◎ 2010 ○ ○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020	◎ 2009 ◎ 2010 ○ ○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020	-DDoS -제로데이 공격 -바이러스, 웜 -웹 공격 -스팸메일 -개인정보침해 -사회공학적 해킹 -불건전정보 유통 -기타 ( )	① 매우높다 ② 높다 ③ 보통 ④ 낮다 ⑤ 매우낮다	① 기술개발 등 기술적 대책 ② 규제 중심의 법제도 개선 ③ 지원, 육성 중심의 법제도 개선 ④ 인식제고 등 사회적 대책	·	◎ 2009 ◎ 2010 ○ ○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020
o 인터넷에서의 국가경계 변화 다양한 이기종(유·무선, 센서등)간의 연결 증가와 인프라 확대로 정보사용자와 저장소의 위치에 따른 문제와 국가간 상이한 규제 및 법률로 인해 분쟁 발생	◎ 2009 ◎ 2010 ○ ○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020	◎ 2009 ◎ 2010 ○ ○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020	-DDoS -제로데이 공격 -바이러스, 웜 -웹 공격 -스팸메일 -개인정보침해 -사회공학적 해킹 -불건전정보 유통 -기타 ( )	① 매우높다 ② 높다 ③ 보통 ④ 낮다 ⑤ 매우낮다	① 기술개발 등 기술적 대책 ② 규제 중심의 법제도 개선 ③ 지원, 육성 중심의 법제도 개선 ④ 인식제고 등 사회적 대책	·	◎ 2009 ◎ 2010 ○ ○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020
o 영상, 모션, 소리 등 미디	◎ 2009 ◎ 2010 ○	◎ 2009 ◎ 2010 ○	-DDoS -제로데이 공	① 매우높다 ② 높다 ③ 보통	① 기술개발 등 기술적 대책	·	◎ 2009 ◎ 2010 ○

어 데이터 증가 모션 인터페이스 등 다양한 인터페이스와 3D미디어 서비스가 증가	○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020	○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020	격 -바이러스, 웜 -웹 공격 -스팸메일 -개인정보침해 -사회공학적 해킹 -불건전정보 유통 -기타 ( )	④ 낮다 ⑤ 매우낮다	② 규제 중심의 법제도 개선 ③ 지원, 육성 중심의 법제도 개선 ④ 인식제고 등 사회적 대책		○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020
o 심리스(seamless) 환경 사물, 시스템에 내제된 센서등의 통신 장치를 통해 시간, 장소에 관계없이 데이터의 저장이나 사용이 끊김없이 지속되는 서비스 환경	◎ 2009 ◎ 2010 ○ ○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020	◎ 2009 ◎ 2010 ○ ○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020	-DDoS -제로데이 공격 -바이러스, 웜 -웹 공격 -스팸메일 -개인정보침해 -사회공학적 해킹 -불건전정보 유통 -기타 ( )	① 매우높다 ② 높다 ③ 보통 ④ 낮다 ⑤ 매우낮다	① 기술개발 등 기술적 대책 ② 규제 중심의 법제도 개선 ③ 지원, 육성 중심의 법제도 개선 ④ 인식제고 등 사회적 대책	.	◎ 2009 ◎ 2010 ○ ○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020
o 대용량 데이터의 집적 다수 정보의 수집으로 대용량 데이터의 집적(ex. 휴대폰을 통해 개인의 하루일과 동안 발생하는 음성 및 주변기기의 대용량 정보 수집 가능)	◎ 2009 ◎ 2010 ○ ○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020	◎ 2009 ◎ 2010 ○ ○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020	-DDoS -제로데이 공격 -바이러스, 웜 -웹 공격 -스팸메일 -개인정보침해 -사회공학적 해킹 -불건전정보 유통 -기타 ( )	① 매우높다 ② 높다 ③ 보통 ④ 낮다 ⑤ 매우낮다	① 기술개발 등 기술적 대책 ② 규제 중심의 법제도 개선 ③ 지원, 육성 중심의 법제도 개선 ④ 인식제고 등 사회적 대책	.	◎ 2009 ◎ 2010 ○ ○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020

o Internet of Things, Internet with Things 'All IP'의 영향으로 물리적공간의 사물에 내제된 네트워크를 통하여 사물간의 컴퓨팅과 커뮤니케이션 능력이 가능해지며 사이버공간과 소통 원활	◎ 2009 ◎ 2010 ○ ○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020	◎ 2009 ◎ 2010 ○ ○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020	-DDoS -제로데이 공격 -바이러스, 웜 -웹 공격 -스팸메일 -개인정보침해 -사회공학적 해킹 -불건전정보 유통 -기타 ( )	① 매우높다 ② 높다 ③ 보통 ④ 낮다 ⑤ 매우낮다	① 기술개발 등 기술적 대책 ② 규제 중심의 법제도 개선 ③ 지원, 육성 중심의 법제도 개선 ④ 인식제고 등 사회적 대책	.	◎ 2009 ◎ 2010 ○ ○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020
o 클라우드 컴퓨팅 환경 저장매체등이 없이도 단말기만을 이용해서 인터넷 이용	◎ 2009 ◎ 2010 ○ ○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020	◎ 2009 ◎ 2010 ○ ○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020	-DDoS -제로데이 공격 -바이러스, 웜 -웹 공격 -스팸메일 -개인정보침해 -사회공학적 해킹 -불건전정보 유통 -기타 ( )	① 매우높다 ② 높다 ③ 보통 ④ 낮다 ⑤ 매우낮다	① 기술개발 등 기술적 대책 ② 규제 중심의 법제도 개선 ③ 지원, 육성 중심의 법제도 개선 ④ 인식제고 등 사회적 대책	.	◎ 2009 ◎ 2010 ○ ○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020
o 개인정보의 경제적 가치 증가 개인정보 및 이동, 사용 이력 상황에 대한 정보등을 수집하고 가공하는 새로운 사업 발생으로 개인 정보의 경제적	◎ 2009 ◎ 2010 ○ ○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020	◎ 2009 ◎ 2010 ○ ○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020	-DDoS -제로데이 공격 -바이러스, 웜 -웹 공격 -스팸메일 -개인정보침해 -사회공학적 해킹 -불건전정보	① 매우높다 ② 높다 ③ 보통 ④ 낮다 ⑤ 매우낮다	① 기술개발 등 기술적 대책 ② 규제 중심의 법제도 개선 ③ 지원, 육성 중심의 법제도 개선 ④ 인식제고 등 사회적 대책	.	◎ 2009 ◎ 2010 ○ ○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020

가치 증가			유통 -기타 ( )				
o 새로운 웹 기반 서비스 경제 활성화 사용자와 판매자 사이의 중간상이 존재가 없어지며 인터넷을 통한 일대일의 소비자 맞춤 형 서비스 활성화	◎ 2009 ◎ 2010 ○ ○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020	◎ 2009 ◎ 2010 ○ ○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020	-DDoS -제로데이 공격 -바이러스, 웜 -웹 공격 -스팸메일 -개인정보침해 -사회공학적 해킹 -불건전정보 유통 -기타 ( )	① 매우높다 ② 높 다 ③ 보 통 ④ 낮 다 ⑤ 매우낮다	① 기술개발 등 기술적 대책 ② 규제 중심의 법제도 개선 ③ 지원, 육성 중심의 법제도 개선 ④ 인식제고 등 사회적 대책	.	◎ 2009 ◎ 2010 ○ ○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020
o 다양한 ID의 존재 각종 서비스를 이용하기 위한 여러 ID의 사용 증가	◎ 2009 ◎ 2010 ○ ○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020	◎ 2009 ◎ 2010 ○ ○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020	-DDoS -제로데이 공격 -바이러스, 웜 -웹 공격 -스팸메일 -개인정보침해 -사회공학적 해킹 -불건전정보 유통 -기타 ( )	① 매우높다 ② 높 다 ③ 보 통 ④ 낮 다 ⑤ 매우낮다	① 기술개발 등 기술적 대책 ② 규제 중심의 법제도 개선 ③ 지원, 육성 중심의 법제도 개선 ④ 인식제고 등 사회적 대책	.	◎ 2009 ◎ 2010 ○ ○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020
o 기술간의 발전속도의 차이 발생 인터넷의 속도, 데이터처리 알고리즘, 데이터의 용량, 저장장치, 보안 등 관련 기술 발전속	◎ 2009 ◎ 2010 ○ ○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020	◎ 2009 ◎ 2010 ○ ○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020	-DDoS -제로데이 공격 -바이러스, 웜 -웹 공격 -스팸메일 -개인정보침해 -사회공학적	① 매우높다 ② 높 다 ③ 보 통 ④ 낮 다 ⑤ 매우낮다	① 기술개발 등 기술적 대책 ② 규제 중심의 법제도 개선 ③ 지원, 육성 중심의 법제도 개선 ④ 인식제고	.	◎ 2009 ◎ 2010 ○ ○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020

도 차이발생			해킹 -불건전정보 유통 -기타 ( )		등 사회적 대책		
o 정보 소통과 통제 기업의 입지 강화를 위해 정보를 독점하려하나 미래 환경에서는 정보소통이 자유로워야 한다. 하지만 정보에 대한 소유권 관리와 통제 필요함	◎ 2009 ◎ 2010 ○ ○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020	◎ 2009 ◎ 2010 ○ ○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020	-DDoS -제로데이 공격 -바이러스, 웜 -웹 공격 -스팸메일 -개인정보침해 -사회공학적 해킹 -불건전정보 유통 -기타 ( )	① 매우높다 ② 높 다 ③ 보 통 ④ 낮 다 ⑤ 매우낮다	① 기술개발 등 기술적 대책 ② 규제 중심의 법제도 개선 ③ 지원, 육성 중심의 법제도 개선 ④ 인식제고 등 사회적 대책	.	◎ 2009 ◎ 2010 ○ ○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020
o 쇼셜 네트워킹의 발전 사이버 공간과 물리적 공간의 경계가 모호해 지고, 사이버 공간의 활동의 증가로 인해 사회적, 윤리적 문제점 발생	◎ 2009 ◎ 2010 ○ ○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020	◎ 2009 ◎ 2010 ○ ○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020	-DDoS -제로데이 공격 -바이러스, 웜 -웹 공격 -스팸메일 -개인정보침해 -사회공학적 해킹 -불건전정보 유통 -기타 ( )	① 매우높다 ② 높 다 ③ 보 통 ④ 낮 다 ⑤ 매우낮다	① 기술개발 등 기술적 대책 ② 규제 중심의 법제도 개선 ③ 지원, 육성 중심의 법제도 개선 ④ 인식제고 등 사회적 대책	.	◎ 2009 ◎ 2010 ○ ○ ○ ○ ◎ 2015 ○ ○ ○ ○ ◎ 2020