ITU 정보보호 전략기획 워크숍 결과보고

장명국 • TTA 표준화본부장

I. 회의 개요

5월20일을 시작으로 22일 폐막한 ITU 정보보호 전략기획 워크숍(ITU New Initiatives Workshop)이 정보화 강국에 상응한 정보보호노력을 강화해야 한다는 인식아래 국제전기통신연합(ITU)과 정보통신부 공동주최로 13개국에서 100여 명의 전문가가 참여한 가운데 개최되었다.

이번 ITU New Initiatives Workshop 개최는 최근 급증하고 있는 주요 정보통신기반에 대한 위협에 효과적으로 대처하기 위한 다양한 국가적 방안이 국가별 사례조사로 발표되었으며, 개별 국가적 노력뿐만 아니라 국제협력이 긴요하다는데 의견을 같이 했다. 그리고 개도국에 대한 지원 제공 등이 제시되었다. 현재 ITU는 선도 연구반을 구성하여 정보보호 분야를 중점적으로 지원 육성하고, 개도국에 대한 정보보호 분야를 집중적으로 관리하기 위하여 이번 회의에서 논의된 내용을 토대로 ITU 이사회에 보고를 통하여 전략적 구축방안을 검토중이다.

양승택 정보통신부장관은 개회식 환영사를 통해 정보보호를 위한 우리정부의 노력을 소개하는 한편, 글로벌 네트워크의 안정적 운영을 위한 국제적 협력이 논의되는 이번 국제회의에 큰 의미를 부여했다. 이어서, 우쓰미(Yoshio Utsumi) ITU 사무총장은 개회사에서 이번 학술회의를 통해 국제적 정보보호 노력을 강화하는 계기가 마련될 수 있기를 희망하였다. 한국의 PC방을 둘러본 사무총장은 세계최고의 시설을 갖추고 있음을 강조하였으며, 직접 e-mail을 점검하고 한국의 PC방에 많은 관심을 보였다.

본 고에서는 3일에 걸쳐 인터컨티넨탈 호텔에서 100여 명이 참가하여 개최된 워크숍 전체개요와 주요 토의내용을 중심으로 관련 내용을 기술하고자 한다.

II. 회의 주요 내용

1. ITU 전략기획 워크숍(New Initiatives Workshop(Creating Trust in Critical Network Infrastructure)

가. Introduction to critical network infrastructures

Critical Network Infrastructure(CNI)에 대해 발표한 이화여대 채기준교수는 CNI의 필요성 및 개념에 대한 설명으로 CNI는 국가기밀 정보나 금융정보를 전송하는 공개 네트워크 또는 사설 네트워크를 의미할 수도 있으며, 중요 정보의 교환을 목적으로 하는 전체 네트워크 또는 부분 네트워크를 의미하기도 하지만 그 개념이 명확하게 정의되어 있지는 않음을 강조하였다. CNI를 구성하는 요소는 피상적으로 나와 있으며 적어도 가용성, 인증, 무결성, 기밀성, 부인방지같은 보안요소들이 요구되어진다. CNI는 크게 외부 망과 완전히 분리된 것과 외부 망과 연결되어 있는 것으로 구별될 수 있으며, 후자가 좀더 일반적이므로 이에 대한 전체적인 접근이 필요하다고 소개했다. 현재 많은 국제기구에서는 체계적인 법적보호를 제공하기 위한 정책들을 준비하고 있으나 CNI 보안에 대한 투자와 표준화가 부족하며, 결론적으로 CNI 보안을 위한 지속적인 연구와 표준화가 수행되어야 하며 CNI 보안시스템의 필요성을 널리 알리는 일이 중요하다고 설명하였다.

나. International Coordination to Increase The Security of CNI

Seymour E. Goodman(Georgia Institute of Technology)은 본 발표를 통해 통신 기반구조 보호를 위한 각국의 공동협력의 필요성을 제시하고 있다. 모든 기반구조는 정보통신 시스템에 대한 의존도가 증가하고 있으며, 이는 국가의 영역을 넘어 세계전역으로 확장되고 있으므로 이러한 의존성은 취약성 증대의 원인이 된다고 지적하면서 기반구조의 보안향상을 위해 관련 기구와 국가들간의 공동협력이 요구된다고 제안하였다. 국제적 노력에 초점을 맞추어 비공식적 두 국가간(Bilateral) 측면, 공식적 두 국가간 측면, 비공식적 다국간(Multilateral) 측면, 공식적 다국간 측면으로 구분하여 공동협력의 이점을 설명하였다. 국제적 공동협력으로써 표준화, 정보공유, 진행중인 공격의 제지, 법적 공동협력, 개발도상국들에 대한 원조지원을 제시하였다. 기반구조를 효과적으로 안전하게 유지하기 위해, 국제적 접근방법이 국가의 전략과 적절히 일치해야 하고 국제적 공동협력은 중요 네트워크 기반구조의 보안성을 향상시키는데 필수적이라고 설명하였다.

다. Creating Trust in Critical Network Infrastructures: Korean Case Study

KAIST 임채호교수는 한국의 CNI(Critical Network Infrastructure)에 대해 다루고 있다. 서두에서는 한국의 지리적, 경제적 환경에 대한 소개를 다루고 있으며, 중반부부터 한국에서의 통신 및 서비스에 대한 통신 기반구조 현황을 서비스 업체를 중심으로 설명하고 있다. 또한 국제적으로 Code Red 및 Nimda와 같은 겹(worm) 공격이 나타나고 있고, 한국에서도 통신 기반구조에 허가되지 않은 침입이나 웜 바이러스(worm virus)같은 인터넷 기반의 공격이 발생하고 있음을 설명하면서 인터넷 웜 공격 및 침입에 대한 통계정보를 제시하였다. 이러한 네트워크 공격을 방지하기 위한 방법으로 주요 정보통신 기반시설을 지정하고, KISA(Korean Information Security Agency), ISAC(Information Sharing and Analysis Centre), 정보보호 지정업체

및 ETRI(Electronics and Telecommunications Research Institute)가 활발하게 취약점 분석 및 평가를 6개월마다 한번씩 수행하여야 하며, 불법적인 공격에 대해서는 법적인 조치가 이루어져야 한다고 제시하고 있다.

라. Creating trust in critical network infrastructure : Brazil case study

Robert Shaw는 브라질의 정보보호와 네트워크 기반구조 보호문제를 해결하기 위한 공공부문과 사설부문에서의 관련 활동들을 소개함. 서두에서는 브라질의 기본적인 국가환경을 소개하고 통계자료를 통해 브라질의 통신환경과 고속 성장률을 유지하고 있는 인터넷 환경을 소개하였다. 브라질에서 인터넷을 통해 국민에게 비용의 절감과 접근의 용이성이라는 이점을 제공하기 위해 2003년까지 인터넷을 통한 모든 서비스 및 정보제공, 전자시민증 구현, 전자지불스킴 구현 등을 목표로 하는 전자정부(e-gov) 프로그램을 수행하고 있음을 소개하였다. 또한, 브라질은 인터넷 서비스 개발촉진을 목표로 정부기관, 백본 운영자, ISP사 대표들로 구성된 브라질인터넷조정위원회, 브라질 인터넷에 연결된 네트워크 관련 행위와 컴퓨터 보안사고 리포트 등을 검토하는 NBSO, 그리고 PKI와 같은 정보의 안전한 인증과 관리에 대한 정책을 개발하는 연방정부 등 정보통신 네트워크의 신뢰성을 보장하기 위한 공공부문과 민간부문의 다양한 활동을 소개하였다. 끝으로 브라질 정부는 정보와 시스템 보호, 사이버 범죄 등에 더 깊은 관심을 가져야 하며, 그로 인해 국민들 또한 네트워크 기반구조에서 필수사항인 신뢰성에 관심을 가져야 할 것이라고 설명하였다.

마. Creating trust in critical network infrastructure : Netherlands case study

Ivo Essenberg는 네덜란드의 컴퓨터 네트워크(통신기반구조) 보호대책에 대한 사례를 주로 다루고 있다. 서두에서는 네덜란드의 정치적, 지리학적, 경제적 환경에 대한 소개와 운송, 공공부문, 수자원 관리부문에 대한 통신 기반구조의 중요성을 네덜란드 통신 기반구조를 책임지고 있는 주요 조직과 함께 소개하였다. 네덜란드는 작은 나라임에도 불구하고 정보사회로서의 발전은 선두에 있다. 보안에 관련된 법을 만들 때 세부적인 것에 치우치기보다는 일반적인 법규를 사용하는 추세이며, 이렇게 함으로써 사회의 변화에 보다 빠르게 대응하여 시대에 뒤떨어지거나 기술적으로 뒤쳐진 법규를 없앨 수 있게 하였다. 2001년 작성된 정책보고서에서는 네덜란드 정보시스템의 신뢰성 증진을 위해 암스테르담 지역에서의 인터넷 사용에 multi-homing기법을 도입하였고, 이 기법을 통해 인터넷 연결이 어느 한 지점에서 실패될 경우 발생되는 문제를 방지함으로써 네덜란드 정부의 네트워크 기반구조의 보안에 있어서 재난을 막을 수 있었고 보다 안전하고 효과적인 통신 기반구조를 확립할 수 있었다고 소개하였다.

III. 맺음말

이번 워크숍에서 ITU 사무총장은 세계최고의 정보통신 인프라를 갖춘 한국은 이에 상응한 정보보호

분야의 연구에 노력하여 줄 것을 지적하였으며, 참석자들은 정보보호 기술개발, 정보기반 보호법 제정 등 한국정부의 노력을 높이 평가하면서 정보화 초일류국의 한국위상을 지속적으로 이어나가기 위해서는 정보보호에 관한 노력 및 관심이 더욱 강화되어야 함을 조언하였다. 또한 ITU에서는 이번 회의에 이어 정보보호 분야에 관심을 갖고 한국사례조사연구팀을 파견하여 국가사회 정보화의 성공사례로서 한국의 초고속망 현황과 정보통신부의 정책전반에 대한 조사결과를 세계 188개 회원국에 널리 홍보할 예정이다.

끝으로 본 워크숍의 성공적인 개최를 위하여 지원하여 주신 정보통신부, 국제전기통신연합, 한국정보보호산업협회, 한국정보보호학회, 한국전자통신연구원, 한국정보보호진흥원, 전자신문사 등에 심심한 감사를 드린다.

한 · 일 생체인식 표준 공조

생체인식 분야의 기술표준화에 대한 업계의 관심이 높아지고 있는 가운데 아시아 국가들의 입장을 대변하기 위한 한 · 일 공조체제가 이뤄질 것으로 보인다. 이에 따라 앞으로 생체인식 표준화와 관련해 한 · 일 두 나라가 아시아 지역은 물론 국제표준화 작업에도 주도적으로 참여할 수 있을 전망이다. 관련업계에 따르면 일본생체인증협회(JBAA)는 최근 한국생체인식포럼(KBA) 관계자에게 공문을 보내 생체인식 분야에서 이슈가 되고 있는 표준화에 대해 서로 협력체계를 갖출 것을 제의했다. 이에 따라 한국생체인식포럼은 5월 13일 한국정보보호진흥원(KISA) 6층 회의실에서 나오히사 코마츠 JBAA 회장을 비롯한 10여 명의 일본 생체인식 연구계 및 업계 관계자들과 회의를 갖고 각국의 표준화 추진동향과 상호 협력방안에 대해 논의하였다. 일본이 이처럼 생체인식 표준화와 관련해 KBA와 공조체제를 갖추려는 것은 생체인식 관련 기술표준을 미국이 사실상 주도하고 있어 공동대응이 필요하다는 판단에서 비롯된 것으로 풀이된다. 실제로 미국은 생체인식 전송표준인 X9.84를 국가표준으로 채택하도록 했으며, 현재 국제표준화기구(ISO)에 국제표준으로 상정한 상태다. 또 디바이스간 호환표준인 BioAPI도 지난 3월 국가표준으로 채택됐다. 이처럼 미국이 생체인식 표준화 부문에서 발빠른 행보를 보이면서 주도권을 잡아나가자 일본은 생체인식 분야에 대한 연구가 비교적 활발한 한국과 행보를 같이하려는 것으로 분석된다. KISA가 중심이 돼 자체 표준을 마련하고 있는데다 BioAPI에 대한 표준 적합성 시험도 예정하고 있는 등 미국 주도의 표준화에 발빠르게 대응하고 있기 때문이다. 생체인식 분야 표준과 관련한 TTA/TC10/SG3 분과에서 활동하고 있는 KISA 김재성 팀장은 이번 회의에서 표준화 및 시험평가소위를 구성하는 방안과 BioAPI에 대한 표준 적합성 시험을 제안하였으며 5월 16일부터 대만에서 열렸던 아시아생체인식워킹그룹(ABWG) 연례회의에서도 이같은 내용을 발표하였다.