通信情報保護學會誌
第 11 券 第 1 號, 2001. 2

초고속국가망의 제도적·관리적 보안대책 방안

이 형 옥

요 약

본 논문에서는 정부에서 추진하고 있는 초고속국가망에서 보안대책을 제도적, 관리적, 기술적 관점에서 분석하고 그에 대한 대책을 제시하였다. 초고속정보통신망사업은 국가정보화를 촉진할 정보인프라 구축에 대한 필요성에 따라 지난 95년부터 추진해온 초고속망구축사업이다. 국가망 구축은 2000년까지 전국 144개 모든 통화권을 고속 대용량(155Mbps~5Gbps)의 광케이블로 연결하였으며, 2000년 7월에는 초고속교환(ATM)서비스를 제공하고 있고, 2000년 말 기준으로 초고속국가망을 이용하는 기관은 28,686개이고 이용회선수는 36,357개 회선 서비스를 제공하고 있는 망이다.

Ⅰ. 서 론

정보통신기술의 급속한 발전에 힘입어 범세계적으로 진행되고 있는 '디지털 혁명'은 과거 산업 혁명시기와는 비교할 수 없는 빠른 속도로 인류의 삶과 생활에 커다란 변화를 가져오고 있다. 인터넷 덕분에 많은 사람들이 손쉽게 정보를 공유하고, 이로 인한 생활의 편익성과 경제성, 효율성 또한 엄청나다.

특히 세계적으로 정보화가 국가경쟁력의 핵심요소로 등장함에 따라, 정부는 21세기 고도정보사회의 기본 인프라가 되는 초고속정보통신망 구축을 위해 1995년 3월에 '초고속정보통신기반구축 종합추진계획'을 수립하여 국가 최우선 사업으로 추진하여 왔다. 그러나 급속하게 발전하는 정보통신 기술 추세와 선진국의 정보화 인프라 구축 동향에 대응하기 위해서는 현실에 적합한 추진계획이 필요하게 되어 1997년 9월에 종합추진계획을 수정·보완하여 목표년도 2015년을 5년 앞당겨 2010년으로 단축하고, 당초 45조원으로 계획했던 소요재원을 약 32조원으로 감축하는 등의 조정 내용이 포함된 '정보통신망 고도화 추진계획'을 수립하게 되었다.

정보통신망 고도화 추진계획은 제1단계사업('95~'97년)의 완료에 따라, 국내 정보통신 가용 자원을 총 점검하고 향후 초고속정보통신망 서비스에 대한 수요전망과 기술 발전 추세 등을 검토하여 실천 가능한 초고속정보통신망사업의 제2단계('98~2002년) 추진계획을 수립하고, 이를 바탕으로 향후 2010년까지의 목표와 소요 재원 등을 전망하였다. 이와 함께 모든 가입자망을 광케이블화 하기로 했던 기존 계획을 수정하여 기술발전 추세와 수요 특성 등을 감안하여 다양한 방법으로 초고속가입자망을 구축할 수 있도록 하는 방안도 포함하였다. 아울러 초고속정보통신망 서비스가 보편화 될 때까지 전화망 등의 기존 통신망을 디지털화 하여 고속·고도화시키고, 우리 나라를 중심으로 한 초고속·대용량의 국제 위성망과 해저 광케이블망 건설을 주도적으로 추진함으로써 급증하는 인터넷 이용에 적절하게 대응하고 고품질의 국제통신 수요를 충족시킬 수 있도록 수정·보완하였다.

한편, 초고속정보통신망 제1단계 사업을 종료하면서 분야별 추진실적 등을 종합적으로 평가·분석한 결과, 초고속정보통신망 구축을 당면한 경제난국을 극복하는 중요한 정책수단으로 활용하고, 보다 효율적이고 경제적으로 추진하기 위해서는 국내·외 기술발전동향, 해외사례, 비용/효과분석 등을 통한 보완·발전이 필요하게 되었다. 이에 따라 1997년 9월 수립한 정보통신망 고도화 추진계획의 사업별 추진목적을 명확히 하고 사업간에 상호연계성을 강화하는 등 이를 보완, 발전시켜 튼튼한 정보대국의 기반을 구축할 수 있도록 1998년 5월 '초고속정보통

* 한국전산원 국가정보화센터 선임연구원(leeok@nca.or.kr)

신망 2단계사업 추진계획'을 수립하였다.

세계는 선진국을 중심으로 하여 정보와 지식이 부가가치 창출의 원천이 되는 지식주도경제 하에서 국가경쟁력 확보를 위해 지식·정보화에 총력을 경주하고 있다. 이에 따라 우리 나라도 '국민의 정부' 임기 내에 21세기 지식·정보화 선진국으로 발돋움 할 수 있는 기틀을 마련하고자 창조적 지식기반국가 건설을 위한 'CYBER KOREA 21' 계획을 1999년 3월에 수립하여 2002년까지 세계 10위권의 지식·정보화 선진국으로 발전하고, 지식기반산업의 GDP 비중을 OECD 수준으로 향상시킬 수 있도록 추진목표를 수립하였다. 이러한 목표 달성을 위해 지식정보사회의 기반이 되는 정보 인프라로서 초고속정보통신망의 조기 구축에 국가적 역량을 집중하고자 2002년까지 당초 6조 4천억원으로 책정되었던 투자재원 규모를 약 10조 4천억원으로 확대·조정하였으며, 이를 위한 세부적인 추진을 위해 초고속정보통신망 2단계사업 추진계획을 연도별 추진실적 및 기술 동향 등을 고려하여 계속해서 보완·추진해 나가고 있다.

최근 인터넷 이용자의 폭발적인 증가와 함께 전자상거래 활성화 등으로 경제·사회 모든 분야에서 정보통신 이용이 급속히 확산되고 있다. 특히, ATM, xDSL 등 급속한 정보통신기술의 발전으로 고속·고품질 서비스 수요가 급속히 증가함에 따라 지식정보사회에 국가경쟁력의 핵심기반을 마련하기 위하여 정보통신망의 조기 고도화의 필요성이 대두되고 있다. 이에 따라 정부는 먼저 당초 2010년까지 구축할 예정이던 초고속정보통신망을 오는 2005년으로 5년 앞당겨 조기에 완성할 계획이다. 이에 따라 초고속망 구축에 소요되는 투자규모가 당초 1995년부터 2010년까지 32조원이었으나 조기구축에 따라 당초보다 약 8조원 늘어난 40조원으로 확정되었다. 우선, 당초의 초고속정보통신망 구축 2단계 사업기간(1998~2002)을 2000년까지 단축하여 초고속정보통신 기간망을 조기에 완성키로 하였다. 이를 위해 전국 144개 주요지역에 대한 광케이블망 구축을 2000년까지 완료하였고, 당초 10Gbps급으로 제공되던 ATM교환기 용량을 40Gbps급으로 확충하여 2000년 7월에 전국적인 초고속 ATM서비스를 실시하였다. 한편, 초고속 가입자망은 광을 비롯하여 xDSL, CATV모뎀, 위성인터넷 등 다양한 방식을 활용하여 고속인터넷 가입자는 1999년 59만명에서 2000년 200만명으로 증가되었고, 초고속국가망 이용기관은 2000년말 현재 이용기관 28,686개, 이용회선수 36,357개 회선을 이용하고 있다.

표 1. 초고속국가망 이용현황(2000.12.31)

단위기관		28,686				계
서비스		전용회선	패킷교환	프레임릴레이	인터넷	
1규격(9.6K)		5,109	3,856	0	0	8,965
2규격(64K)		9,981	332	1,256	415	11,984
3규격	256K	0	0	0	3,135	3,135
	512K	5,223	5	468	1,899	7,595
	2M	4,885	3	221	1,447	6,556
4규격(45M)		97	0	0	23	120
5규격(155M)		5	0	0	0	5
계		23,297	4,196	1,945	6,919	36,357

초고속정보통신망은 정부·기업의 생산성과 경쟁력을 높이는 21세기 가장 중요한 인프라로 앞으로 초고속망과 정보기술을 이용한 정부와 기업 정보화가 더욱 가속화될 것이다. 특히 정부는 정보기술을 활용한 정부업무 혁신과 온라인 민원처리에 중점을 두어 추진할 방침이다. 세계 최고의 초고속인터넷 보급율을 바탕으로 국내 온라인콘텐츠, 소프트웨어, e비즈니스 등 인터넷 신산업분야가 세계적인 경쟁력을 갖춰 21세기 중추 산업으로 성장할 수 있을 것으로 보인다. 아울러 초고속망 구축을 통해 축적된 세계적 기술력은 해외로 수출되고 있으며 특히 아파트용으로 개발된 xDSL계열의 장비들은 경쟁력을 갖추고 있어 많은 수출이 기대된다. 또한 향후에는 초고속정보통신망에서 문서교환, 상거래 및 다양한 응용서비스 등이 이뤄지는 만큼 정보보호분야 기반 구축과 국민들간 새로운 정보윤리를 확립·확산하는 일이 새로운 과제로 떠오르고 있다.

본 논문에서는 먼저 제 외국의 정보통신망 보안대책과 관련하여 미국, 일본의 현황을 알아본다. 또한, 정부에서 추진하고 있는 초고속국가망에서의 보안대책을 제도적, 관리적, 기술적 관점에서 문제점과 현황을 알아보고, 그에 대한 대책을 제시하였다.

Ⅱ. 국외의 초고속정보통신망 보안대책

2.1 미국의 정보통신망 보안대책 동향

미국은 1988년 대통령령인 PDD-63 발표 이후

에 주요 기반 구조에 대한 보호대책 수립에 착수하였다. 미국의 정보통신망 보안에 관련된 법·제도로는 FCC, 전기통신법에 관한 연방규약, 전기통신에 관한 연방규약, 행정명령, PDD-63 등이 있다.

FCC는 의회의 직접적인 책임 하에 있는 미연방의 독립된 기관이며, 라디오, 텔레비젼, 유선, 위성 등 국가간 통신을 조절하는 임무를 수행하고 있다. FCC에서 정한 법규는 50개 주와 콜롬비아 자치주 및 미국의 귀속영토에 효력이 미치며, FCC는 10개의 분야로 나누어 작업을 추진하고 있다. FCC에서 제정한 법중 비상경보시스템(EAS)은 국가적 비상사태가 발생했을 때 대통령이 국민들에게 알리기 위한 기능을 제공하는 시스템이다.

PDD-63은 PCCIP의 권고에 따라 만들어졌으며, 1997년 10월 PCCIP는 전기통신, 금융, 에너지, 운송 및 필수 정부 서비스와 같은 상호 연결된 기반구조에 대한 보호대책을 요구하였다. PDD-63은 이러한 권고를 면밀히 검토한 후 주요기반구조 보호에 대하여 2003년까지 신뢰성 있고 안전한 정보시스템 구조를 구축하고, 2000년까지 고도로 향상된 보안기능을 정보시스템에 구축하는 목표를 가지고 있다.

미국 정부는 새로운 기술을 적용하기 위한 선도적 역할 및 신기술 개발과 사용의 문제점들을 해결하는 역할을 하며, 새로운 시스템과 응용 서비스들의 도입에 따른 정책 입안자와 정부관리들에게 정보의 비밀과 보안 분야에 대한 새로운 필요성을 느끼게 하였다. 이에 상무부는 통신망과 관련한 기술 및 보안절차 개발을 위하여 상무성내에 NIST를 설치하였으며, NIST는 정보기술 시스템과 통신망의 보안을 개선하기 위한 기술과 시험절차를 개발하기 위해 산업체와 협력하여 작업을 수행하고 있으며, 미 정부내에서 NIST는 정보기술 보안에 대하여 선도적인 역할을 하고 있다. 백악관에서는 NII의 관리자로서의 위치를 확고히 하기 위해 IITF를 만들었으며, IITF는 공공기관과 민간분야의 서로 다른 의견을 하나로 이끌어내며, 정부기관으로 하여금 그들의 정책을 좀더 빠르고 효과적으로 수행해 나갈 수 있도록 하고 있다. IITF에는 3개의 위원회가 설립되었으며 통신정책, 정보정책, 응용기술 등을 주관한다.

1996년에는 클린턴 대통령의 지시로 정보전쟁에 관한 특별위원회(PCCIP)를 구성하였으며, 이 위원회는 국가 기반구조 특히 정보통신 기반을 보호하는 것을 최우선 과제로 수행하고 있다.

미국의 기술적 보안대책과 관련하여서는 PDD-63을 통하여 미국의 상호 연결된 공중통신망과 사설통신망에 대한 보안을 위하여 국가적 노력을 기울일 것을 요구하였으며, 이에 따라 GSA에서도 FTS 보호프로그램을 개발하여 운영 중에 있다.

FTS 보호프로그램은 테러분자에 의한 공격, 주요기반시설에 대한 공격, 사이버공간상의 공격 등을 포함한 위협으로부터 국가의 방위력을 증강하는데 필요한 전문서비스와 제품들을 제공하기 위하여 OIS에서 만들어졌다.

MISSI를 구성하고 있는 보안 시스템은 워크스테이션 보안과 시스템/국지영역 보안시스템이다. 워크스테이션 보안시스템은 Fortezza 암호화 PC 카드를 이용하여 전자우편, 전자상거래 등의 서비스를 제공하기 위한 응용프로그램으로 구성되며, 시스템/국지영역 보안시스템은 국지 영역 내에 상주하면서 국지 영역과 외부 망간에 액세스 제어와 암호화 서비스를 제공한다.

통신망 암호 시스템으로는 X.25 계층이나 IEEE 802.3 계층에서 패킷을 암호화하기 위한 NES, ATM에서 셀을 암호화하기 위한 장비인 FASTLANE과 ATM/IP를 기반으로 하는 전술 통신망에서 다중등급보안을 제공하기 위한 TACLANE, SONET과 호환 가능한 암호기인 KG-189가 있다.

미국의 통신사업자중의 하나인 Pacific Bell의 재난복구 계획은 조직내의 어떠한 주요사업 파괴의 영향으로부터 회복하기 위한 절차를 수립한것이며, 재난에 대하여 미리 준비하는 경우 재난으로부터 생존할 수 있다는 것을 보여 주고 있다. 재난복구 계획은 주요통신 자원은 고객, 주요 공급자, 고용원 집단간의 통신, 사무실간의 통신, 투자자나 외부 통신 등에 초점을 맞추고 이들과의 통신 보장을 위한 재난복구 대책을 세우고 있다. 그러나 실제로는 이러한 재난복구 계획보다는 평상시의 꾸준한 훈련과 개선이 중요하며, 직원들의 상시교육 이외에도 재난이 발생하였다고 가정한 모의 훈련을 정기적으로 실시하고 있다.

2.2 일본의 정보통신망 보안대책 동향

일본 정부는 정보통신을 성장시키기 위하여 기존 통신사업자의 통신망에 새로운 망 사업자가 쉽게 연결할 수 있게 하는 정책을 펴고 있으며, 이로 인하여 통신망 사업자가 크게 증가함으로써 통신망에 대

한 보안대책이 필요하게 되었다. 인터넷을 이용한 전자상거래 시 상대방을 인증하고 통신 내용이 도중에 변경되지 않도록하기 위해 통신 당사자 이외의 제 3의 기관(인증기관)이 거래 당사자의 본인 성명과 통신 내용의 진실성을 증명하도록 하였다.

일본 정부에서는 전자상거래의 보급 등 컴퓨터의 이용이 국민생활 및 경제 전반에 걸쳐 널리 확대되고 동시에 정보통신망 환경의 급속한 발전으로 인하여 1997년 1월 1일에 정보통신망의 보안대책을 수립하기 위하여 정보처리진흥사업협회(IPA) 내에 "보안센터"를 설립하였다. "보안센터"는 각각의 행정부서에서 별도로 수행하던 컴퓨터 바이러스의 피해 신고, 부전 액세스의 피해 신고, 암호 기술 개발 등의 업무를 효율적으로 처리하기 위하여 설립되었다.

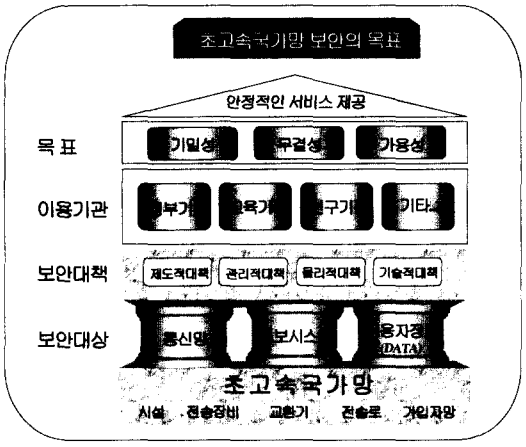
일본의 물리적 관리적인 보안대책안을 살펴보면, 통신망의 불법 침입 요소를 통신망의 사용자 측면과 제공자 측면을 고려하여 구분짓고 있으며, 불법 침입에 대비하여 암호를 관리하고 사용자를 확인 할 수 있는 시스템과 침입차단 시스템을 연구 개발하여 정보보호정책 수립 시 고려해야 할 사항으로 정의하고 있다. 또한, 바이러스에 대비하여 최근 동향을 파악하고, 바이러스 방지를 위해 기술 개발과 바이러스 관련 자문기관을 두어 범 국민적으로 대처 할 수 있는 능력을 배양하고 있다. 더불어 통신망 제공자가 수행할 수 있는 보안대책을 제시하여 사용자로 하여금 통신망 사용에 불편이 없으면서 신뢰성 있는 통신망을 사용할 수 있도록 하고 있다.

일본의 기술적인 보안대책과 관련해서는 다른 나라와 유사하게 진행되고 있다. 해킹 및 컴퓨터 바이러스에 대한 기술적 대책으로는 암호화, 인증 기술, 침입차단시스템 등을 들 수 있다. 특히, 최근에는 전자화폐와 전자상거래에 대한 관심이 높아지면서 보안 대처기술의 방향이 암호화와 인증 기술에 집중되어지는 경향을 보이고 있으며, 이를 위한 개인정보의 보호 및 부정액세스, 바이러스 대처에 대한 연구개발도 진행 중에 있다.

Ⅲ. 초고속국가망의 보안대책 필요성

국가 및 공공부문의 정보화 진전으로 정보통신시스템에 대한 의존도가 증가하고 있어, 주요 국가망 이용기관의 정보시스템에 문제가 발생하면 국가 사회적인 기능이 마비되어 막대한 경제적 손실뿐만 아니라 사회 혼란 초래 가능성 마저 있어 이에 따른 보안성 확보의 중요성이 부각되고 있다. 또한, 국가기밀정보나 국민 신상정보 등을 취급하는 국가망 이용기관에 대한 기밀성을 제공하고, 정보통신서비스의 신뢰성을 높이기 위해 별도의 초고속국가망 보안대책에 대한 필요성이 대두되고 있다.

초고속국가망 서비스는 국가 및 지방자치단체 등 총 28,686기관이 36,357회선 서비스를 제공(2000년 12월말 현재)하고 있어, 국가 및 공공기관 등에 대한 보편적 서비스로 자리잡고 있으나, 아직 국가망사업자 및 이용기관에 대한 별도의 보안대책 없이



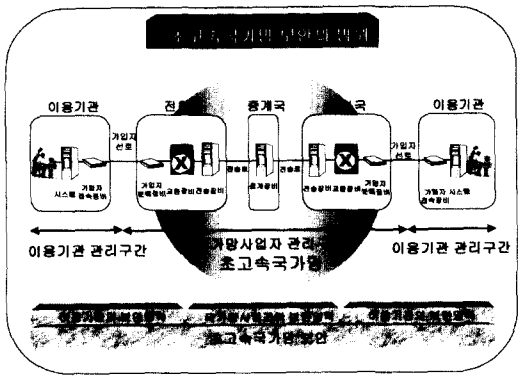
공중망 수준으로 운영하고 있는 실정이다. 따라서 초고속국가망 이용기관에 대한 기밀성을 제공하고, 국가비상사태 및 재난·재해나 기밀정보의 유출방지를 위한 물리적, 관리적, 기술적인 대책 마련이 요구된다 하겠다.

초고속국가망의 목표는 초고속국가망을 이용하는 국가망 이용기관에게 전쟁 및 재난·재해 등 국가비상사태 시에도 보안의 기본목표인 비밀성(Confidentiality)·무결성(Integrity)·가용성(Availability)을 확보한 안정적인 서비스를 제공하고자한다. 보안의 기본목표에 대한 용어 정의는 다음과 같다.

- 무결성(Integrity) : 정보처리 과정 및 전송도중에 정보가 불법적으로 변경되지 않고 일관성을 유지하는 것.
- 가용성(Availability) : 사용자가 시스템으로부터 필요한 정보를 필요한때에 항상 접근하여 사용할 수 있게 하는 것으로, 침해사례는 전산기 파괴, 통신망 단절, 컴퓨터 바이러스 등이 해당된다.
- 비밀성(Confidentiality) : 암호 등을 이용해

제 삼자가 전송자료의 내용, 출처, 목적지, 횟수, 길이 등을 알지 못하도록 하는 것.

- 인증성(Authenticity) : 특정시스템이나 사용자가 정당한 사용자인가를 확인하는 것으로 예를 들어 패스워드나 디지털서명 등이 있다.



초고속국가망은 서비스를 제공하는 국가망사업자와 국가망을 이용하는 이용기관으로 나눌 수 있다. 초고속국가망에서 국가망 이용기관 및 국가망사업자의 보안책임은 "국가정보통신보안기본지침(국정원)"에 의해 해당기관의 장에게 있다. 이에 본 논문의 보안대책은 국가망사업자의 준수사항을 중심으로 제도적, 관리적, 물리적, 기술적인 분야로 구분하여 알아보도록 한다.

Ⅳ. 초고속국가망 보안관리 현황 및 문제점

4.1 제도적 분야

초고속국가망 사업자들은 "국가정보원"이나 "정보통신부"의 지침이나 법률에 근거하여 자체적인 보안지침을 보유하고 있으나 보안지침은 시설, 설비, 인원 등의 보안관리에 치중되어 있는 실정이다. 초고속국가망 사업자들은 기존의 공중망 비상계획 및 재해 복구 지침을 보유하고 있으나 실제상황을 가정한 훈련은 을지훈련 등에 한정되어 있는 상태이다. 초고속국가망 사업자는 기존의 공중망의 보안관련 연도별 활동계획을 수립하여 이행여부를 년 1회 이상 점검하고 있으나, 보안관련 연도별 활동계획이 주로 시설, 장비, 인원 보안에 치중하고 있으며 기술적인 전산보안 분야에 대한 활동계획 수립 및 이행 여부 확인은 다소 미흡한 현실이다.

4.2 운용관리 분야

문서, 시설, 인원, 전산 및 통신 분야의 보안관리자는 별도로 지정되어 있고, 보안관리자에 대해 관리적인 측면의 교육은 잘 이루어지고 있으나, 정보통신의 기술변화 싸이클이 너무나 짧아 기술적인 측면의 보안교육은 다소 미흡한 상태이다. 특히, 초고속국가망 사업자들의 고장 및 장애 발생과 관련한 대책 안은 다음과 같다.

초고속국가망 사업자들은 서비스 중단에 대비하여 이중전송 및 우회경로 확보 등의 방법을 사용하여 안정적인 서비스 제공을 준비하고 있다. 예를 들어 한국통신은 서비스 중단시 우회경로를 이용하고 있고, 데이콤은 백본망을 링 형태로 구성해 정보를 이중 전송을 실시하고 있다. 이와 관련하여 국가망사업자가 이용자로부터 서비스 장애신고를 접수하면 관련장비를 이용하여 장애를 점검해 조치하고 있다. 장애접수 후 한국통신은 3시간, 데이콤은 1시간 이내에 장애 처리가 이루어지지 않으면 보상을 원칙으로 하고 있다. 국가망 사업자들의 자체 회선에 대한 서비스 중단 및 장애발생시의 보고 및 처리 절차는 마련되어 잘 관리되고 있으나, 국가망사업자간에 연동되는 구간인 경우에는 정식적인 협조체제가 마련되어 있지 않아 장애 발생 시 해결을 위해 향후 대책이 요구된다.

또한, 교환 및 전송장비 자체에 대한 보안 취약점은 현재까지는 없는 것으로 알려져 있지만, 교환 및 전송장비를 관리하는 전산관리시스템이 중앙집중방식이거나 구역별로 집중화되어 있어 전산관리 시스템을 통한 외부의 불법침입 가능성에 대한 보안 문제 야기에 대해서는 가능성이 상존 하고 있다.

4.3 시설관리 분야

초고속국가망 장비가 있는 사옥 및 시설에 대한 출입통제는 제한구역과 통제구역으로 지정해 철저히 관리되고 있다. 예를 들면, 통제구역 출입 시에는 사전에 통보하고 관리자의 허락을 받도록 하고 있으며, 통제구역 출입 시 출입자관리대장 작성을 하도록 하고, 초고속국가망 시설 및 장비 감시를 위한 CCTV, Card Key 등이 설치되어 외부인의 출입을 통제하고 있으며, 초고속국가망 설비의 보호를 위한 항온 항습기 및 UPS 등이 설치되어 운영되고 있다.

4.4 기술적 분야

전송장비의 기술적인 위협요인은 없으며, 전송매체에 대한 도청 등의 위협요인이 학술적으로 논의되고 있으나 현실적으로 고려해 볼 때 우려할 정도의 수준은 아니다. 기밀정보 등의 송·수신은 이용기관 차원의 암호화 방법을 채택해서 해결 가능하고, 전송매체의 인위적, 환경적 요인에 의한 훼손에 대해서는 장애점검 및 회선점검 등을 통해 유지 및 관리되고 있다. 이미 언급한 바와 같이 교환기 경우에는 교환기를 조작하는 별도의 언어를 사용하므로 일반인들의 조작이 불가능하므로 자체의 보안 위협요인은 없다. 그렇지만 교환기를 운용·관리하는 전산관리시스템이 통합 관리되고 있어 기술적으로 교환기의 해킹 가능성이 있다. 특히, HINET-P, DNS 등 X.25 공중망을 이용하는 경우 사용자간 CUG를 구성·운영하고 있어 해킹 가능성은 있지만, CUG의 관리가 철저하여 현실적으로 보안 문제는 없는 것으로 파악되고 있다.

V. 초고속국가망의 보안대책 방법

초고속국가망의 보안대책을 크게 단기적인 방향과 장기적인 방향으로 나누어서 제시하였다. 먼저 단기적인 방향에 대하여 제도적, 운영 관리적, 시설 및 기술적인 분야에 대해 알아본다.

5.1 제도적 분야

초고속국가망 사업자는 기존의 공중망 보안대책과 구별되는 초고속국가망 사업자용 지침을 수립하여 시행하고, 현업의 실무담당자를 대상으로 지침에 대한 교육 실시, 초고속국가망 연도별 활동계획 수립 및 이행여부를 점검하여야 할 것이다. 기술적인 전산 보안분야에 대해서는 향후 산·학·연의 공동연구를 통해 문제점을 도출하고 이에 대한 대응책을 초고속국가망 사업자용 보안지침에 보강하도록 한다. 또한, 초고속국가망 사업자용 지침에 사업자 차원의 주기적인 기술적 보안점검 실시를 명시하여 보안사고를 예방할 수 있도록 조치하여야 할 것이다.

5.2 운영관리 분야

장애 발생시 신속한 복구 및 장애처리를 위하여 사업자간 정식 협조체제를 마련하여 운영하도록 하고, 현업의 전산 및 통신 보안관리자를 대상으로 기술적인 보안 교육을 년 1회 이상 실시하여 현업 보안담당자들의 보안관련 기술변화에 능동적으로 대체할 수 있는 환경을 조성해야 할 것이다.

또한, 초고속국가망 구성요소를 관리하는 전산관리시스템, 영업 및 장애관리 등 주요 전산시스템에 대한 사업자 차원의 주기적인 기술적 보안점검을 실시하여 운영 관리적 측면에서 보안의 문제점을 사전에 예방하도록 하여야 할 것이다.

5.3 기술적인 분야

전송매체의 인위적, 환경적 유실상태를 조기에 감지할 수 있는 망관리시스템(NMS)을 도입하여 전송매체를 실시간 시스템으로 관리 할 수 있도록 사업자 시스템을 구축하고, 사업자간의 연동 시스템을 통하여 관련 정보를 상호간에 교환 할 수 있도록 하여야 할 것이다.

국가 및 공공기관에 대해 보안성을 확보하기 위해 ATM교환서비스에서 VP Tunneling 기능을 적용하여 기관의 성격상 보안성을 요구하는 기관에 보안성을 확보할 수 있도록 하여야 할 것이다. 또한 초고속국가망을 구성하는 교환기 및 전송로를 운용·관리하는 전산관리시스템 사업자의 주기적인 기술적 보안점검을 실시하여야 한다.

5.4 장기적 방향

정보통신 분야의 기술적인 추세를 반영하여, 초고속국가망 사업자용 보안 지침의 지속적인 보완 작업을 실시하도록 하여, 최소 2년 단위로 지침의 보완 작업을 실시한다. 정보통신부의 보안감사에 초고속국가망 보안점검 분야를 포함하도록 하고, 필요시 국가정보원의 지원을 받도록 하여야한다. 사업자 차원의 초고속국가망 구성 요소(예, 전송매체, 전송망, 교환망, 전산시스템 등)에 대한 보안 취약점 분석 및 대응책 마련에 관한 연구를 실시하여 대응방안을 수립하도록 하여야 한다.

통신위성을 통한 정보전송에 대한 기술적인 보안을 위해 정보 암호화 기법을 도입하는 대책을 수립하여야 할 것이다. 초고속국가망 시설 및 장비를 대상으로 위험분석을 실시하여 위협요소를 도출하고 대응책을 마련할 수 있도록 하고, 초고속국가망 시

설·장비·운용관리시스템에 위험관리 개념을 도입하여 체계적으로 관리하는 방안을 강구하여야 할 것이다.

또한 초고속국가망 보안 지침내에 정보전에 대비한 보안대책 분야를 포함하여 대 북한 정보전에 대비한 보안대책 및 선진국의 국내정보 유출에 대비한 보안대책 등이 포함되어야 할 것이다.

Ⅵ. 결 론

초고속정보통신망은 정부·기업 및 사회 전반의 생산성과 경쟁력을 높이는 21세기 가장 중요한 인프라로 자리 매김 되고 있다. 최근 인터넷의 확산으로 인터넷을 이용한 업무가 날로 증가하고 있으며, 이를 뒷받침하기 위한 정보통신에 대해서도 기술적인 연구가 많이 진행 중에 있다. 그러나, 초고속 인터넷 서비스 수요의 증가만큼 정보를 이용하는 생활의 변화가 동반하지만 그의 역기능 또한 증가하고 있어 사회적인 문제를 야기하는 사례가 점차 증가하고 있다. 이러한 문제들은 개인의 사생활 침해뿐만 아니라 더 나아가서는 국가 사회 질서조차 위협하는 형태로 나타나고 있다.

국가에서 추진하고 있는 초고속국가망은 전국의 28,000여 개의 공공기관이 접속하여 서비스를 이용하고 있으므로, 각 기관이 갖고 있는 데이터나 정보의 흐름에 대해서는 완벽한 보호가 이루어져야한다. 즉, 초고속국가망 이용자에게 초고속국가망에서의 보안에 대해서는 신뢰감을 주어야만 초고속국가망의 운용면에서 성공하게 될 것이다. 이를 위하여 본 논문에서는 국가망사업자가 지켜야할 보안대책에 대하여 제도적, 관리적, 운영적 및 기술적인 분야에 대하여 분석하고 그에 대한 대책안을 제시하였다.

참 고 문 헌

[1] 초고속정보통신기반구축종합추진계획, 정보통신부, 1995.

[2] 정보통신망고도화추진계획, 정보통신부, 1997.

[3] 초고속국가망 보안대책 수립을 위한 국·내외 동향조사 및 연구, 한국전산원, 1999.

[4] 초고속국가망 보안 취약점 분석 및 대응 방안 연구, 한국전산원, 2000.

[5] http://www.pccip.gov/summary.html, PCCIP Report Summary.

[6] http://nsi.org/Library/Compsec/nii.txt, NII Security "The Federal Role".

[7] http://iitf.nist.gov/about.html, About the President's Information Infrastructure Task Force.

〈著者紹介〉

이 형 옥 (Hyeong Ok Lee)

1996년 3월~1999년 8월 : 전남대학교 전산학과(시간강사)

1999년 2월 : 전남대학교 전산통계학과(이학박사)

1999년 10월~현재 : 한국전산원 국가정보화센터(선임연구원)