通信情報保護學會誌
第6卷 第3號, 1996. 9

초고속정보통신기반하에서 시큐리티 프레임워크

(Security Framework on the Information Superhighway)

박 정 현*

요 약

초고속정보통신기반이 구축되면 보다 다양한 서비스 출현이 예상되고 이에 따른 위험 및 취약요인도 증대하게 될 것이다. 따라서 보다 안전한 응용서비스 공급과 이용자 보호 및 올바른 초고속정보통신기반의 발전을 위해서는 초고속정보통신기반하에서 요구되는 종합적인 시큐리티 대책의 수립이 필요하다. 본 논문에서는 초고속정보통신기반의 시큐리티 위협요인과 필요한 시큐리티 서비스를 살펴보고 초고속정보통신기반 요구되는 시큐리티 요구사항과 시큐리티 기본원칙을 제시한 후 시큐리티 프레임워크와 시큐리티 대책 방향을 제안하였다.

1. 서 론

가속화되는 정보통신기술의 발달은 정보화 사회의 촉진을 유도하면서 초고속정보통신기반구축으로 이어지고 있다. 초고속정보통신기반이 구축되면 우리의 일상생활에 큰 변화를 가져오게되어 가정/직장/정부에서의 업무효율을 향상시키고, 생활의 질을 높여주며 국가경쟁력을 강화시켜주는 순기능적 기여가 예상되나 한편으로는 법죄적, 사회적, 문화적, 윤리적 측면의 역기능을 예견케 한다. 이러한 역기능 영향을 줄이기 위한 대책으로 사회적 변화에 따른 안전성을 사전에 충분히 점검하고 초고속정보통신기반 구축 계획과 서비스 제공 일정등을 고려하여 적기에 시큐리티 대책을 확보하기 위한 방안을 수립해야 한다. 더우기 정보고속도로를 구축하는 세계적인 추세에 통신망의 지능화, 고속화, 광대역화, 대규모화, 개방화와 유선망, 이동망, 위성망, 방송망등 개별망의 통합화를 바탕으로 하는 초고속정보통신망에서 정보의 손실/파괴/변조에 따른 각종 안전사고와 시스템의 신뢰성에 대한 문제는 향후 초고속정보통신기반의 발전에 큰 영향을 주게 될것이 분명하다.

미국에서는 NII(National Information Infrastructure)의 성공적인 구축을 위하여 NII Security Issue Forum 통해 시큐리티 확보를 추구하고 있으며 유럽의 OECD(Organization For Economic Co-operation And Development)에서도 시스템 시큐리티을 위한 기본원칙등을 제정하고 있는 실정이다.

본 논문에서는 초고속정보통신기반하에서 종합적으로 수립되어야할 시큐리티 대책에 기본적으로 필요한 시큐리티 프레임워크를 논의

* 한국전자통신연구소 초고속망연구실

하고자 한다. 이에 먼저 초고속정보통신기반과 이에 따른 시큐리티 위협요인을 2장에서 살펴보고, 초고속정보통신기반하에서 요구되는 기본적인 시큐리티 요구사항과 시큐리티 서비스를 3장에서 제시하였다. 이를 바탕으로 시큐리티 프레임워크를 4장에서 제안 하였고, 제안된 시큐리티 프레임워크를 추진하기 위한 시큐리티 대책방향과 정부의 역할을 아울러 5장에서 살펴본다.

2. 초고속정보통신기반과 시큐리티 위협요인

2.1 초고속정보통신기반이란?

○ 초고속이란? = 차세대 기술을 의미[2]
- 기술의 고도화 (ATM 기술, 광전송, 교환기술, 광대역 CDMA, 음성처리기술, 영상압축·복원기술, 정보저장/검색기술, DB기술, 객체지향 S/W기술, 초고속 프로세서 기술, S/W개발환경기술, ASIC 기술, 광소자기술, GUI 기술 등)
- 정보전송 및 처리의 고속화 (교환/전송/단말)
- 서비스의 다양화와 서비스 이용의 편리성이 전제된 상태
- 지능화/멀티미디어화
- 개인화/인간화

○ 정보통신기반이란? 정보의 빠른 전달과 처리의 신속화, 정보저장/유통의 고급화, 정보이용의 편리화를 제공하는 각종 통신기반 (네트워크, 교환기, 컴퓨터, S/W, H/W, DB, 시스템등이 포함한 환경을 의미

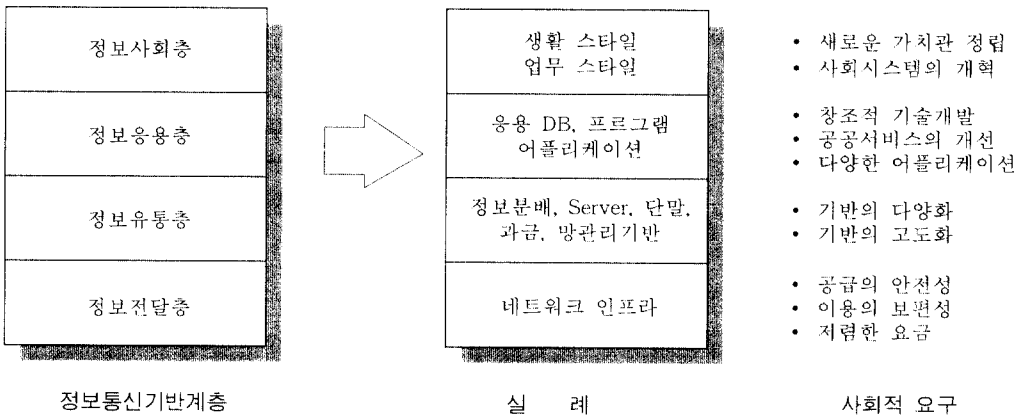
○ 초고속정보통신기반이란? 고속통신망 (Internet, Public switchednetwork, Cable, Wireless, Satellite Communications, 기타공중망/사설망을 모두 포함), DB, 고급컴퓨터 등에 의해 전자 정보를 접속/처리/저장/전달할 수 있게 하는 시스템으로 이용자는 필요에 따라 원하는 형태의 정보를 시간제약 없이 언제, 어디서나 신속하게 창출/유통/이용할 수 있는 환경을 말한다. 이와같은 환경하에 보다 많은 통신망간의 상호접속이 이루어 질때 개인/회사/정부는 멀티미디어 통신형태로 KII를 이용하게 되며, 특별히 전자상거래/공유 정보 분배/정부서비스 및 혜택의 수신에 보다 많이 KII를 이용하게 된다.

○ 초고속정보통신기반 구조[2]
(그림 1)은 초고속 정보 통신 기반 구조를 나타낸다.

2.2 시큐리티 위협요인

○ 사전적 의미의 시큐리티는? 사전적인 의미로 시큐리티는 안전/보안/보호/방위/방어/보증으로 설명 된다. 여기서 안전은 편하고 아무탈이 없음 혹은 위험이 없음을 의미하며 보안은 안전을 유지함, 보호는 잘 돌보아주고 지켜줌으로 설명된다. 영어로는 Security는 Safety, Freedom from danger, Given as guaramtee를 의미하고 Safety는 The state of being safe(안전/무사), Protection은 The state of protecting or being protected, a person or thing that protects to keep safe from danger, enemies, attack(보호/보안)을 의미한다.

○ 법률적 의미로 정보화 촉진기본법 제 1장 제 2조 4항에서 정의하는 정보보호란 정보의 수집/가공/저장/검색/송신/수신중에 정보의 훼손/변조/유물등을 방지하기 위해 관리적/기술적 수단 (정보보호 시스템)을 강구하는 것을 말한다.



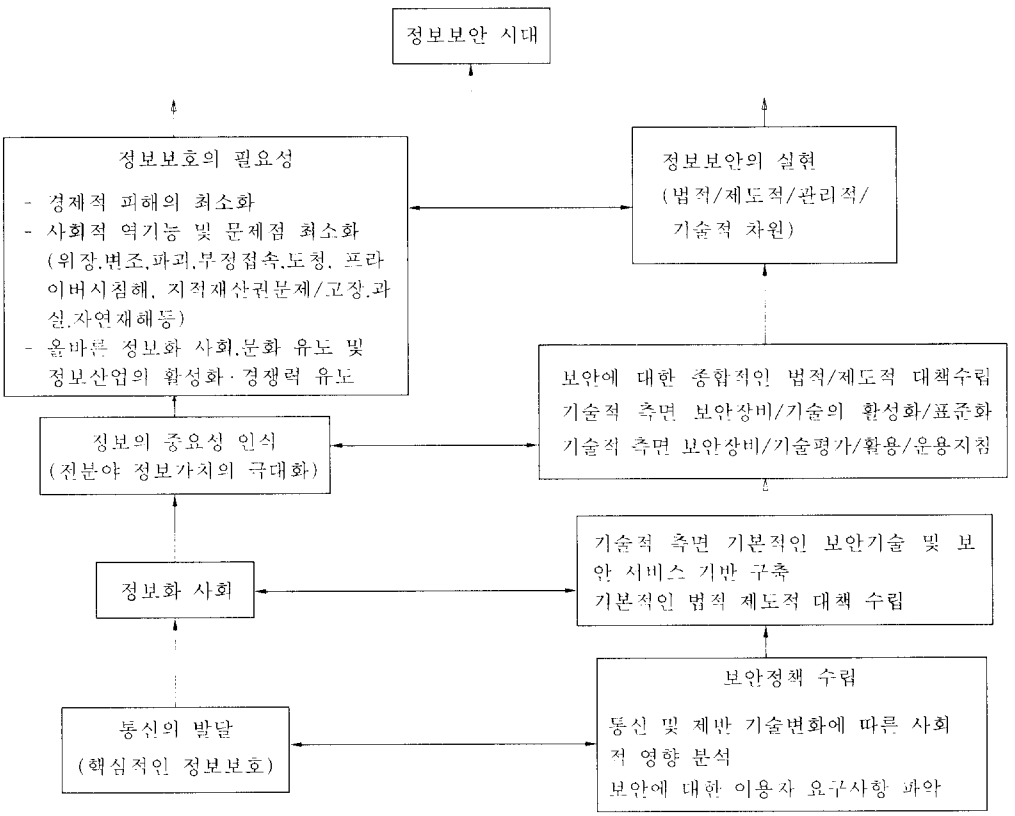
(그림 1) 초고속정보통신기반 구조

○ 미국에서는 정보보호를 데이타 및 시스템을 고의적으로 혹은 실수에 의한 불법적인 공개/변조/파괴등으로 부터 보호라 하고, 영국 및 유럽에서는 전자적인 형태의 정보를 처리/저장/통신의 모든 단계에 걸쳐서 보호하는 것으로 정의하고 있다.[3]

○ 초고속정보통신기반하에서 안전, 보안, 정보보호 혹은 시큐리티(Security)란?
정보(개인/회사/정부)가 우연 혹은 악의에 의해 변조되거나 파괴되는것을 막고, 시스템(컴퓨터/네트워크/하드웨어/DB/소프트웨어(O/S 및 응용 S/W등)/기타 정보관련 장비및 시설)이 일정 품질 수준을 유지하면서 지속적으로 수행되고, 정보와 통신 서비스 등이 언제든지 이용할 수 있도록 하며, 정보가 적정사람에게만 접속하고 비밀을 유지 할수 있게 하는 것을 의미하는 것으로 무결성/비밀성/신뢰성/유용성을 보장 및 유지하는 것을 말한다.

○ 초고속정보통신기반하에서 시큐리티 대책 필요성
통신망과 통신기술에 기초한 통신기반의 변화, 서비스의 다양화/고급화/지능화/전자화, 그외 KII (korea Information Infrastructure)/GII(Global Information Infrastructure)를 기반으로한 다양한 전자정보 및 국제 전자통신 서비스 출현과 이에 따른 시큐리티 측면에서의 변화는 향후 초고속정보통신기반의 발전에 크게 좌우할 시큐리티 대책의 필요성을 설명하기에 충분하다. 이를 도식적으로 표현하면 (그림 2)와 같다.

○ 시큐리티 위협요인
시큐리티의 주요 목적은 인가되지 않은 사람이 정보 및 시스템에 접근하거나 인가없이 정보를 사용/오용/파괴하는 것을 방지하는 것이며 그밖에 광의의 개념에서는 고장이나 자연 재난으로부터 정보 및 시스템을 보호하는 것을 포함한다. 초고속정보통신기반하에서 예상되는 시큐리티 위협요소는 환경 변화(전산망의 국내외적 상호 연동/사용자 급증/불특정 사용자 증대/다양한 전자통신 서비스 출현과 각 서비스별 요구되는 보안 기술 미흡 등)로 더욱 다양한 형태로 나타날것이고, 그 취약성 또한 증대되어 이를 위한 시큐리티 서비스도 더욱 강화되어야 한다. 보안을 위협하는 요인은 크게 두가지로 볼 수 있는데 하나는 정



(그림 2) 초고속정보통신기반하에서 안전성 배경과 필요성

보 및 시스템의 노출과 부정한 접속에 따른 사람에 의한 인위적인 위협요인과 고장 및 자연재해로 인한 자연적인 위협요인이다. 여기서 정보 및 시스템의 부정한 접속과 이에 따른 문제점, 그밖에 고장 및 자연재해로 인한 자연적인 위협요소로는 다음 사항들이 고려될 수 있다.

① 부정한 접속 형태의 공격적 위협요소
- 위조(Forgery : Documents or Records)
- 사기(Fraud : 권한자의 특권 도용) 혹은 가장(Masquerading : Steal Access Right, Duplicate Address, Impersonation)
- 도난 (Theft : Information, System, Service)
- 트로이 목마 (Trojan Horses)
- 트랩도어 (Trap Door)
- Sabotage
- Tempest
- Wiretapping (도청)
- Eavesdropping
- Leakage
- 공모
- 정보 및 시스템의 잘못 사용
- 정보 및 시스템의 고의적인 유출
- 파기/폭파/방화
- 컴퓨터 바이러스

② 부정한 접속 및 데이타 노출에 따른 문제점
- 변조(추가/삭제/순서변경/재연/지연)
- 복사
- 정보 및 시스템의 파괴
- 부정한 이용

③ 고장으로 인한 시큐리티 위협 요소
- 시스템 운영 및 활용 미숙
- 정보 및 시스템 관리 소홀
- 설계 오류 및 S/W 버그
- 고장 및 시스템 오동작/오접속

④ 자연적 위협 요소
- 화재/홍수
- 지진/폭풍
- 낙뢰/부실 장비 및 시설

⑤ 파생되는 역기능
- 프라이버시 침해
- 지적재산권 문제
- 시스템 비정상 운영 및 경영 악화
- 국민 및 국가 경제 손실 초래
- 사회 질서 및 윤리 파괴
- 기타

3. 시큐리티 요구사항과 시큐리티 서비스

시큐리티는 정보화 사회에서 개인/회사/정부의 경제적 피해를 최소화 할 수 있는 수단이며 국가 경제와 사회 전반적인 역기능과 문제점을 해결할 수 있는 중요한 대안이라 볼 때, 향후 초고속정보통신기반의 발전을 좌우하게 될 것이다. 더우기 초고속정보통신기반이 구축되면 다양한 응용서비스가 출현할 것이고 이에 따른 시큐리티 위협 요인과 취약성이 증대하게 되어 보다 종합적이면서도 체계적인 시큐리티 대책이 수립/시행되지 않으면 상당한 혼란과 피해, 시행착오를 예상케 한다. 본 소절에서는 초고속정보통신기반에서 시큐리티 종합 대책 수립에 반드시 고려되야 할 기본적인 시큐리티 요구사항과 시큐리티 서비스를 제시한다.

3.1 초고속정보통신기반하에서 시큐리티 요구사항

○ 기본적인 요구사항

초고속 정보 통신 기반하에서 기본적으로 요구되는 시큐리티 요구사항은 정보와 시스템에 대해 비밀성/무결성/유용성/신뢰성 이다.

① 비밀성(Confidentiality)
정보/시스템이 적정 사람에게만 접속하고 이용하며 비밀을 유지할 수 있게 하는 것

② 무결성(Integrity)
정보가 우연 혹은 악의에 의해 변조되거나 파괴되는 것으로 부터 막을 수 있게 하는 것

③ 유용성(Availability)
정보/통신서비스/시스템이 언제든지 이용할 수 있는 상태

④ 신뢰성(Reliability)
정보/서비스/시스템이 일정 품질 수준을 유지하면서 지속적으로 수행 할 수 있는 상태

○ 시큐리티에 대한 이용자/서비스 공급자 요구사항

초고속정보통신기반하에서 이용자/서비스 공급자 측면의 요구사항은 크게 다음과 같은 범위의 응용서비스에 대한 기술적/법적 시큐리티 대책으로 볼 수 있다.

① 상업적 서비스에 대한 보안 대책(오락/게임/소프트웨어/컴퓨터 산업에서의 지적 재산권 보호를 위한 준비)
② 보험/금융/재정 정보에 대한 보안 대책
③ 보건/건강/의료 정보에 대한 보안 대책
④ 교육 정보에 대한 보안 대책
⑤ 정부서비스와 정부정보의 전자배달에 대한 보안 대책
⑥ 지능 교통/운송 관리 정보/시스템에 대

한 보안 대책
⑦ 무역 정보를 위한 보안 대책
⑧ 공중 통신망과 인터넷을 중심으로한 KII 기반의 유용성과 신뢰성 대책

○ 시큐리티 기본 원칙 수립
다음과 같은 시큐리티 기본 원칙과 이에 대한 법적/기술적 준비도 요구된다.

① 정보를 볼수 있고, 없고를 통제할 수 있도록 해야함
② 필요한 상황에 따라 통신 상대를 알 수 있게 해야함
③ 저장된 혹은 전송된 정보가 변조되었는지를 알수 있도록 해야함
④ 정보와 통신 서비스가 언제 유용한지, 언제 유용치 않는지를 알수 있도록 해야함
⑤ 원치 않은 정보나 침입자를 막을 수 있도록 해야함

○ 정보에 대한 기본 원칙 수립
그밖에 정보에 대해 아래 원칙을 수용하고 이를 위한 법적/기술적 준비가 있어야 한다.

① 수집 제한이 원칙
② 정보내용의 원칙
③ 목적 명확화의 원칙
④ 이용제한의 원칙
⑤ 안전보호의 원칙
⑥ 공개의 원칙
⑦ 개인 참여의 원칙
⑧ 책임의 원칙(이용자/소유자/제공자)

○ 기타 고려사항

① 개인/회사/정부 정보의 2차적 사용에 대한 기술적/법적 통제 능력
② 정보의 손실/부정한 접속/부정한 이용에 대한 기술적/법적 대책
③ 개인/회사 정보의 정부 이용에 대한 불신 문제 대책
④ 외부침입자로 부터의 자신의 시스템 및 정보를 보호할 수 있도록 하는 기술적/법적 대책
⑤ 중요한 시기 시스템 장애/손상에 대한 대책
⑥ 개인정보(재정상태/건강/구매습관등) 노출 및 조작 문제등에 대한 대책

3.2 시큐리티 서비스

시큐리티 정책수립에서 다루어야 하는 시큐리티 기술/서비스는 초고속정보통신기반하에서 예상되는 여러가지 역기능 요인과 다양한 응용서비스들을 고려하여 제공되어야 한다. 아래에서는 초고속정보통신기반하에서 시큐리티 위협요소에 대처하기 위한 기본적인 시큐리티 기술/서비스로써 고려될 수 있는 사항들을 제시한다.

○ 인증(무결성)
송신자(사용자/클라이언트)A는 수신자(시스템/서버)B에게 자신이 A임을 설명할 수 있으나 임의의 제 3 자 X가 B에게 자신이 A임을 가장하여 설명할 수 없게 하는 기술이다. 일반적으로 인증은 사용자 인증과 메세지 인증으로 나눌 수 있으며 정보의 변경/조작 여부를 확인하는 형태로 이루어지는 메세지 인증은 무결성 서비스를 지원하며, 사용자 인증은 정당한 사용자 인지를 확인하는 서비스로 정보시스템에서 정보의 생성/전송/처리/기억/판단등의 행위에 관여한 올바른 사용자를 보증하는 서비스이다.

○ 서명(부인봉쇄)
송신자(사용자/클라이어트)A는 수신자(시스템/서버)B에게 자신이 A임을 설명할 수 있으나 임의의 제 3자 X가 B에게 자신이

A임을 가장하여 설명할 수 없고, B도 자신에게 혹은 또 다른 제 3자 C에게 자신이 A임을 설명할 수 없게 하는 기술이다. 서명은 기본적으로 메세지 인증과 식별(사용자 인증)의 서비스를 포함하여 송.수신 부인봉쇄 서비스를 지원하는 보안 기술이다. 기술적 접근은 상대의 공개키로 1차 메세지를 암호화하고 자신의 비밀키로 2차 암호화해서 보낸 후, 수신자는 먼저 상대의 공개키로 복호화한 후 자신의 비밀키로 2차 복호화를 하는 방식이 있고 여기에 one way hash function을 결합해서 보다 간결하고 강화된 서명 스킴을 만들 수 있다.

○ 식별(접근제어)

송신자(사용자/클라이언트)A는 수신자(시스템/서버)B에게 자신이 A임을 설명할 수 있으나 임의의 제 3 자 X가 B에게 자신이 A임을 가장하여 설명할 수 없고, B도 또 다른 제 3자 C에게 자신이 A임을 설명할 수 없게 하는 기술이다. 패스워드/카드키/사용자 개인특성 및 소유정보를 기반으로 접근제어를 관리하는 사용자 접근 제어와 정보/시스템 비밀 분류 등급 기준과 정보/서비스에 대한 사용자의 접근제어 기준을 바탕으로 룰 기반 접근제어 기술을 기초로 하는 정보/서비스 접근제어(강제적/차등적/역할 기반 접근제어)가 있다. 따라서 정보나 시스템에 대한 사용자 접근을 제어하는 식별은 서명이나 인증에서의 사용자 인증의 개념을 포함하고 있다. 멀티로그인 및 멀티 세션등과 같은 형태로 카드나 패스워드, Firewall, 사용자 특징을 통해 정보나 시스템(DB/응용환경/시스템/네트워크등)접근을 통제하는 단방향 사용자 식별 및 접근제어가 있고, KERBEROS등을 이용하여 네트워크 접속 통제를 하는 양방향 식별 혹은 인증 방식이 있다.

○ 암호(비밀성)

암호는 정보의 비밀성을 유지하도록 하는 기술로 기본적으로 정보나 시스템의 노출에 대한 비밀 보호서비스를 제공한다. 또 정보가 노출된다 하여도 키가 없는 한 그 정보의 의미를 알 수 없도록 하는 이 암호 기술은 기본적으로 비밀키 방식과 공개키 방식으로 지원 된다. 비밀키 방식은 송/수신자간에 같은 키를 비밀리에 소유한 후, 메세지 암호화/복호화시 사용하는 방식이고(DES : Data Encryption Standard),공개키 방식은 송/수신자간에 별도의 암호화/복호화 키를 소유하고 메세지 전송시만 서로간에 공통키를 소유하여 송/수신하거나 공개된 암호화 키로 암호화하여 복호화 키를 갖고 있는 사람많이 복호화 할 수 있도록 하는 형태(RSA : Rivest, Shamir, and Adleman)가 있다.

○ 감사

정보와 시스템 보호에 대한 관리적 측면의 보안 서비스로, 보안의 위협이 권한 받은 내부요인, 비권한된 내부요인, 권한된 외부요인, 비권한된 외부요인 형태 순으로 이루어 진다고 볼때 효과적이고 체계적인 물리적 감사외에 정보와 시스템에 대한 논리적 감사 기술은 반드시 필요한 보안 서비스라 하겠다. 논리적 감사 기술로는 정보 및 시스템 사용에 대한 추적 기술과 로깅화일 감사를 통한 방법이 있다.

○ 자동복제 관리기술(지적재산권)

각종 전자정보(오락/게임/SW/기타 컴퓨터 서비스)의 복사에 대한 보호를 제공하는 서비스로 지적재산권 문제를 해결해주는 보호기술을 의미하며 자동복제 관리시스템을 들 수 있다.

○ 프라이버시 보호 기술

앞에서 기술한 보호기술을 바탕으로 이루어지는 보호서비스로, 특별히 개인 정보 보호를 위해 활용할 수 있는 보호기술을 의미한다. 주로 비밀성/무결성을 보장하는 보호기술이 개발되어 프라이버시 보호를 위한 보편적인 공통 보호기술로 활용될 수 있다.

○ 정보 중복 및 분산 기술(유용성/신뢰성)

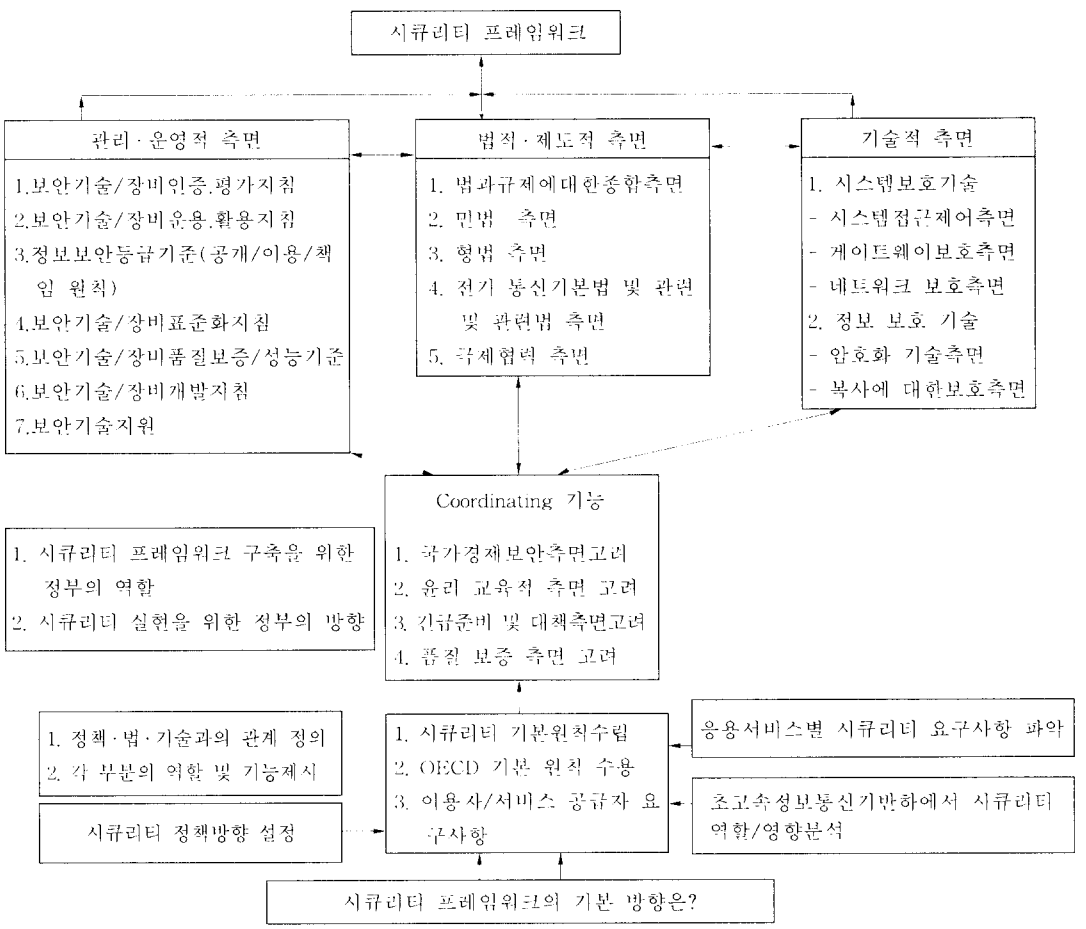
컴퓨터와 통신상에서 정보의 중복과 이중화를 지원할 수 있는 기술과 이의 효율적이고 체계적인 관리 기법을 의미하며 정보에 대한 유용성과 신뢰성을 지원하는 서비스이다.

○ 시스템 이중화(유용성/신뢰성)

시스템의 이중화를 지원하는 기술과 이의 효율적이고 안전한 운영/관리 기법을 의미하며 시스템에 대한 유용성과 신뢰성을 지원하는 서비스이다.

4. 초고속정보통신기반하에서 시큐리티프레임워크

초고속정보통신기반하에서 정의되야할 시큐리티 프레임 워크는 기본적으로 1차적 보호에 활용될 기술적/운영/관리적 차원과 2차적 보호에 활용될 법/제도적 차원으로 고려 할 수



(그림 3) 시큐리티 프레임워크

있으며 이들은 상호 연관되어 수립 되어야 할 것이다. 그림3은 초고속정보통신기반하에서 수립되어야 할 기본적인 시큐리티 프레임워크로 고려할 수 있다.

5. 시큐리티 대책 방향

초고속정보통신기반하에서 수립되어야할 시큐리티 대책 방향은 먼저 응용서비스별 시큐리티 요구사항을 파악하고, 시큐리티 기본원칙과 정보와 시스템에 대한 기본원칙을 정의하여 시큐리티 프레임워크를 설정하는 것이다. 그리고 시큐리티 프레임워크를 바탕으로 서로간의 역할을 정립하고 법적/제도적 측면의 통제와 시행에 대한 준비와 기술적/관리적 측면의 준비를 하는 것이다. 앞에서 제시된 초고속정보통신기반하에서 수립되어야할 시큐리티 프레임워크를 확립하는데 있어 보다 구체적인 시큐리티 대책 방향 제시가 요구되며 이를 추진하기 위한 정부의 역할이 무엇보다도 중요하다 하겠다. 본 소절에서는 시큐리티 프레임워크를 확립하기 위한 구체적인 시큐리티 대책 방향과 정부의 역할을 살펴 본다.

5.1 Coordinating 기능 정의

시큐리티 역할과 프레임워크를 기본 바탕으로 서로간의 역할 정립을 정의하는 Coordinating 기능은 초고속 정보통신기반하에서 다음과 같은 사항이 고려되어야 한다.,

- ○ 국가 경제/보안 측면
- ○ 윤리/교육적 측면
- ○ 비상 준비/대응 측면
- ○ 품질 보증 측면

5.2 법적/제도적 통제와 시행준비

초고속정보통신기반하에서 발생 가능한 여러 문제점과 역기능에 이용자를 보호할 수 있는 최종적 대책인 법적 측면은 크게 다음과 같은 측면에서 고려되어야 한다.

- ○ 초고속정보통신기반하에서 관련된 종합적인 법적/제도적 규제와 시행 측면 제시(전기통신법/컴퓨터프로그램보호법/저작권법/기타 전기/통신/방송/유선/무선 관련 법/제도)
- ○ 민법 측면
- ○ 형법 측면
- ○ 국제 협력 측면

5.3 기술적/관리적 대책 준비

시큐리티에 있어 가장 기본적이며 확실한 대처 준비는 기술적 측면이라 할 수 있는데 초고속정보통신기반하에서 시큐리티 대책 수립에 필요한 기술적 요인은 크게 시스템 측면과 정보 측면으로 고려 할 수 있다.

- ○ 시스템 보호 측면
  - 시스템 접근제어
    (패스워드/개인식별/인증/감사)
  - 게이트웨이 보호(Firewall)
  - 시스템/네트워크 보호
    (신뢰성/시큐리티:이중화)

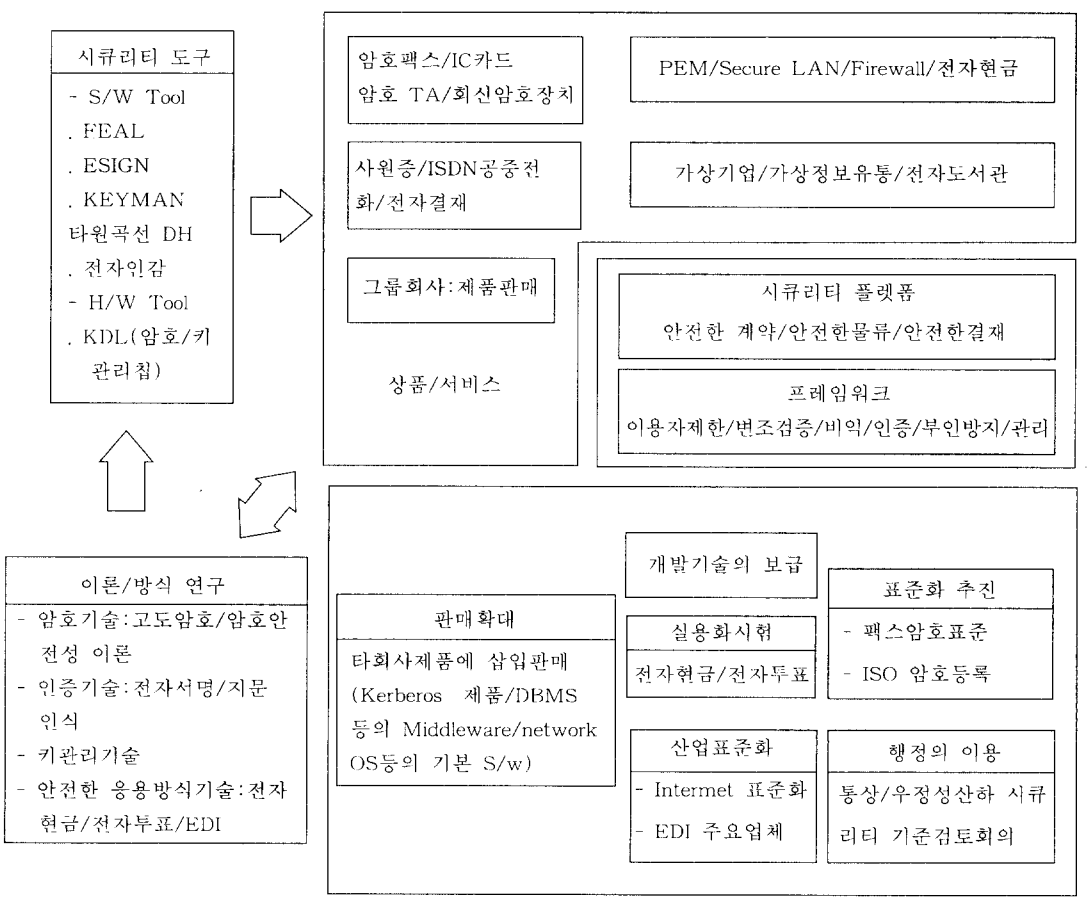
- ○ 정보 보호 측면
  - 정보 접근제어
    (패스워드/개인식별/인증/암호/감사/분산/백업)
  - 복사에 대한 보호(자동복제관리시스템)

시스템과 정보의 기술적 보호에서는 앞에서 언급한 보안서비스가 다중 형태로 적용 되도록 고려해야 할 것이다. (그림 4)는 기술적 차원의 시큐리티 대책 흐름[5]을 일본의 예로 보여준다.

5.4 시큐리티 대책 추진을 위한 정부 역할

앞에서 제시한 시큐리티 대책 방향을 종합적이고 구체적으로 진행하고, 초고속정보통신기반하에서 요구되는 시큐리티 실현하는데는 정부의 역할이 무엇보다도 중요하다 하겠다. 안전한 초고속정보통신기반을 구축하여 보편적이고 일반적인 전자통신서비스를 제공하고 모든 이용자에게 편리한 정보 통신 환경을 제공하기 위해 정부는 다음과 같은 역할을 해야 할 것이다. 먼저 KII의 민간활동을 증진하는 시설 지원자 혹은 촉진자로서 역할, 대중 이익 및 일반 복지 보호자로서 역할, 중요 연구분야에 대한 자금지원과 민간분야에 필요한 기술개발 지원자로서의 역할, 그리고 마지막으로 KII를 실현하기 위해서는 각 역할에 따른 필요한 준비가 있어야 하겠다.

○ KII의 민간활동을 증진하는 시설 지원자 혹은 촉진자로서 역할



(그림 4) 시큐리티 기술적 대책 흐름(일본 NTT)

- 시큐리티 위협요인 증대 인식과 이의 해결책의 필요성 인식고취
- 시큐리티에 대한 이용자 요구사항 파악을 바탕으로 정보 및 시스템에 대한 시큐리티 기본원칙 수립
- KII에 유용한 보안 장비와 기술의 개발 보급
- 신뢰성있고 안전한 고품질 보안 장비/보안기술의 민간 개발 유도

○ 대중 이익 및 일반 복지 보호자로서 역할
- KII에서의 적절한 비상 대처 능력 준비
- KII에 맞는 법적/제도적 통제
- KII 환경에 맞는 각종 법적 준비
- KII/GII 환경에 따른 국제적 대처 준비

○ 중요 연구 분야에 대한 자금지원과 민간분야에 필요한 기술 개발 지원자로서 역할

○ KII 이용자로서 역할과 정부 정보의 보호 및 책임
- 정부정보에 대한 적절한 관리과정 수립과 보안 요구사항 수행
- 정부의 보안비상 능력 준비
- 보안기술/장비의 신뢰성/시큐리티
- 정부에서 필요한 보안 기술 기반 구축

이밖에 정부는 국가 경제와 국민보호 차원에서 법적/제도적/관리적/기술적 측면에서 필요한 시큐리티 프레임워크 설정과 실현에 있어 적절한 역할을 정의하고 보완하여 지속적으로 추진해야 할 것이다.

6. 결 론

초고속정보통신기반의 발전을 좌우할 시큐리티는 그 대책을 수립하는데 있어 먼저 이용자와 서비스 제공자의 시큐리티 요구사항을 파악하는 것이 가장 중요하다. 이용자와 서비스 제공자의 시큐리티 요구사항을 파악하는데 있어서는 KII상에서 가장많이 이용될 전사상업 서비스(게임/오락/소프트웨어/기타 컴퓨터 서비스등)에 대한 사항, 금융/재정/보험 관련 서비스에 대한 사항, 의료/건강/보건에 관련된사항, 교육 서비스에 관련된 사항, 교통/운송 서비스에 관련된 사항, 무역/경제 서비스에 관련된 사항, 그리고 공중망과 인터넷에 대한 신뢰성 사항을 검토하는 것이 기본적이라 할 수 있으나 다양하게 출현될 응용서비스 형태로 나누어 보다 구체적으로 조사하는 것이 중요하고 정확할 것이다. 또한 KII에서 필요한 시큐리티 기본원칙 수립과 이를 바탕으로 시큐리티 대책의 기본요소인 법/제도/기술/관리 사항이 종합적으로 표현된 시큐리티 프레임워크와 역할정립은 초고속정보통신기반하에서 시큐리티 대책이 진행되야할 방향이라 하겠다. 특히, 초고속정보통신기반하에서 더욱 다양해지는 시큐리티 위협/취약 요인에 1차적으로 대응할 기술적 대책에 있어서는 크게는 시스템보호와 정보보호 측면이 고려될 수 있으나 필요한 응용 서비스별 새로운 보안기술/서비스의 개발과 보급이 초고속정보통신환경에서의 서비스 이용자 폭을 넓히는 지름길이라 할 수 있다. 그리고 올바른 시큐리티 프레임워크 설정과 대책 수립, 이를 추진하기 위한 정부의 역할 정의 및 수행은 초고속정보통신기반하에서 필요한 보안 정책의 핵심사항이라 하겠다.

참 고 문 헌

[1] David J. Stang, Sylvia Moon, "Network Security Secrets", IDG Books Worldwide, Inc., 1993

[2] 김수창외 2인 "초고속정보통신기반 구축 전망", ETRI 주간기술동향, 1995. 6

[3] 이순주 "금융전산망 정보보호 현황 및 향후 전망", '96 전산 보안 세미나, 1996. 3

[4] 김광조, "보안시스템의 최근 기술 동향", NETSEC-KR '96, 1996. 5

[5] 박정현, 이준원 "초고속정보통신기반하에서 시큐리티 요구사항", AIN '96, 1996

[6] Shamir, "Identity-Based Cryptosystems and Signature Schemes", Proc.of Crypto '84,1984

[7] Gary S. Morris, "Computer Security and the Law", GSM Associates, 1996

[8] Timothy D Schoechel, "Privacy on the Information Superhighway", CyberLYNX

[9] Rick Nevins "AMP, Incorporated Network Security", Global IT Infrastructure, 1996

□ 著者紹介

박 정 현

Senior Engineer, Imformation Infrastructure Network section at ETRI in Korea (1982.3-Present).

M.S, Soongsil Graduate School (Electronics Engineering Department) in Korea (1985).

B.S, Soongsil University (Electronics Engineering Department) in Korea (1982).

Research interest : Security protocol, Cryptology, Satellite communication.