

□특집□

# 초고속정보통신기반에서의 안전성 대책방향과 정부 역할

박 정 현<sup>†</sup> 이 상 호<sup>††</sup>

◆ 목 차 ◆

- |                    |             |
|--------------------|-------------|
| 1. 서 론             | 5 시큐리티 서비스  |
| 2. 초고속정보통신기반과 시큐리티 | 6 안정성 대책 방향 |
| 3. 시큐리티 위협요소와 문제점  | 7. 정부의 역할   |
| 4. Secure NII 요구사항 | 8. 결 론      |

## 요 약

초고속정보통신기반이 구축되면 보다 다양한 서비스 출현이 예상되고 이에 따른 위협 및 취약 요인도 증대하게 될 것이다. 따라서 보다 안전한 응용서비스 공급과 이용자 보호 및 올바른 초고속정보통신기반의 발전을 위해서는 초고속정보통신기반하에서 요구되는 종합적인 안전성 대책의 수립이 필요하다. 본 논문에서는 초고속정보통신기반의 안전성 위협 요인과 필요한 시큐리티 서비스를 살펴보고 초고속정보통신기반 요구되는 안전성 요구사항과 안전성 기본원칙을 제시한후 안전성 대책방향과 정부의 역할을 제안한다.

## 1. 서 론

가속화되는 정보통신기술의 발달은 정보화사회의 축진을 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 범죄적, 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 안전성 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 정보

† 정회원 · 한국전자통신연구원 초고속정보통신연구  
본부 선임연구원

†† 정회원 충북대학교 컴퓨터과학과 교수

의 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 안전성 확보를 추구하고 있으며 유럽의 OECD (Organization For Economic Co-Operation And Development)에서도 시스템 안전성을 위한 기본원칙등을 제정하고 있는 실정이다.

본 논문에서는 초고속정보통신기반하에서 종합적인 안전성 대책 수립시 기본적으로 필요한 안전성 요구사항과 그 대책 방향, 그리고 정부의 역할을 제안한다. 이에 먼저 초고속정보통신기반과 시큐리티를 정의한후, 안전성 위협요소과 문제점을 3장에서 살펴본다. 이어 초고속정보통신기반하에서 요구되는 기본적인 안전성 요구사항을 4장에서, 시큐리티 서비스를 5장에서 각각 제시하였다. 이를 바탕으로 안전성 대책방향과 정부의 역할을 6장과 7장에서 제안한다.

## 2. 초고속정보통신기반과 시큐리티

### 2.1 초고속정보통신기반이란 ?

#### ● 초고속정보통신기반이란 ?

고속통신망 (Internet, Public switched network, Cable, Wireless, Satellite Communication, 기타공중망/사설망을 모두 포함), DB, 고급 컴퓨터등에 의해 전자 정보를 접속/처리/저장/전달할 수 있게 하는 시스템으로 이용자는 필요에 따라 원하는 형태의 정보를 시간제약 없이 언제, 어디서나 신속하게 창출/유통/이용 할 수 있는 환경을 말한다. 이와같은 환경하에 보다 많은 통신망간의 상호접속이 이루어 질때 개인/회사/정부는 멀티미디어 통신 형태로 NII를 이용하게 되며, 특별히 전자상거래/공유 정보 분배/정부 서비스 및 혜택의 수신에 보다 많이 NII를 이용하게 된다.

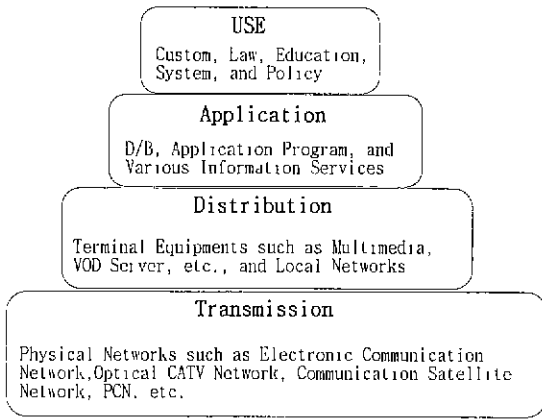
#### ● 초고속정보통신기반 구조

아래 그림 1과 2는 각각 초고속정보통신기반의 구조적 개념과 개념적 모델을 나타내 본것이다.

### 2.2 시큐리티

Information Infrastructure Layer	Layer	Objectives
Sence of value of life (laws and regulations)	4th layer	Life style Work style
Education, medical, administrative, informationizing of industry systems	3rd layer	Application database Application database
Distribution of information	2nd layer	Information distribution functions Transmitting/receiving equipment
Physical information transmission equipment	1st layer	Network infrastructure

(그림 1) 초고속정보통신기반의 구조적 개념



(그림 2) 초고속정보통신기반의 개념적 모델

● 초고속정보통신기반하에서 안전 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/W 등)/기타 정보관련 장비 및 시설)이 일정 품질 수준을 유지하면서 지속적으로 수행되고, 정보와 통신 서비스 등이 언제든지 이용할 수 있도록 하며, 정보가 적정사람에게만 접속하고 비밀을 유지 할 수 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 NII/GII를 기반으로한 다양한 전자정보 및 국제 전자 통신 서비스 출현과 이에 따른 안전성 측면에서의 변화등은 초고속정보통신기반의 올바른 발전 방향을 검토하는데 있어 기본적인 사항이라 하겠다. 이들 변화에 따른 각종 역기능과 문제점을 최소화하고 초고속정보통신기반의 순기능적 역할이 올바르게 발전되기 위해서는 시큐리티에 대한 종합적인 대책이 강구되어야 할것이다.

### 3. 시큐리티 위협요소와 문제점

#### 3.1 시큐리티 위협 요소

보안을 위협하는 요인은 크게 정보 및 시스템의 노출과 부정한 접속에 따른 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.

● 부정한 접속 형태의 공격적 위협 요인

- 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

- 파괴/폭파/방화

- 컴퓨터 바이러스

● 고장으로 인한 안전성 위협 요인

- 시스템 운영 및 활용 미숙

- 정보 및 시스템 관리 소홀

- 설계 오류 및 S/W 버그

- 고장 및 시스템 오동작/오접속

● 자연적 위협 요인

- 화재/홍수

- 지진/폭풍
- 낙뢰/부실 장비 및 시설

### 3.2 문제점

- ① 부정확한 접속 및 데이터 노출에 따른 문제점
  - 변조 (추가/삭제/순서변경/재연/지연)
  - 복사
  - 정보 및 시스템의 파괴
  - 부정확한 이용
- ② 파생되는 역기능
  - 프라이버시 침해
  - 지적재산권 문제
  - 시스템 운영 및 경영 악화
  - 국민 및 국가 경제 손실 초래
    - 사회 질서 및 윤리 파괴와 기타 문제

## 4. Secure NII 요구사항

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

### 4.1 기본적인 안전성 요구사항

- ① 비밀성(Confidentiality)  
정보/시스템이 적정 사람에게만 접속하고 이

용하며 비밀을 유지할 수 있는 상태

- ② 무결성(Integrity)  
정보가 우연 혹은 악의에 의해 변조되거나 파괴되는 것으로 부터 막을 수 있는 상태
- 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

### 4.2 응용서비스별 시큐리티에 대한 이용자/서비스 공급자 요구사항

- ① NII에서 상업에 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 대한 보안 대책
- ⑦ 무역 정보를 위한 보안 대책
- ⑧ 공중통신망과 인터넷을 중심으로한 NII 기반의 유용성과 신뢰성 대책

### 4.3 NII보안을 위한 기본 원칙 수립(법적/관리적/기술적 준비 요구)

- 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 알 수 있도록 해야함

- ① 정보와 통신 서비스가 언제 유용한지, 언제 유용치 않는지를 알수 있도록 해야함
- ① 원치 않은 정보나 침입자를 막을 수 있도록 해야함

#### 4.4 정보에 대한 기본 원칙 수립

초고속정보통신기반에서는 다음과 같이 정보에 대한 기본원칙이 법적/관리적/기술적으로 준비되어야 한다.

- ① 수집 제한의 원칙
- ① 정보내용의 원칙
- ① 목적 명확화의 원칙
- ① 이용제한의 원칙
- ① 안전보호의 원칙
- ① 공개의 원칙
- ① 개인 참여의 원칙
- ① 책임의 원칙 (이용자/소유자/제공자)

#### 4.5 기타 고려사항

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

#### 5. 시큐리티 서비스

시큐리티 정책수립에서 다루어야 하는 시큐리티 기술 및 서비스는 초고속정보통신기반 하에서

예상되는 여러가지 역기능 요인과 다양한 응용서비스들을 고려하여 제공되어야 한다. 아래에서는 초고속정보통신기반하에서 시큐리티 위협요소에 대처하기 위한 기본적인 시큐리티 기술 및 서비스로서 고려될 수 있는 사항들을 제시한다.

#### ① 인증

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.

기술적 접근은 비밀키 공유를 통한 간접인 인증과 세션키 공유를 통한 직·간접 인증 등이 있고 one way hash function을 통한 메세지 다이제스트 및 인증이 있다.

#### ① 서명

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 자신에게 혹은 또 다른 제 3 자 C에게 자신이 A임을 설명할 수 없게 하는 기술이다.

서명은 기본적으로 메세지 인증과 식별(사용자 인증)의 서비스를 포함하며 송·수신 부인봉쇄 서비스를 지원하는 보안 기술이다. 기술적 접근은 상대의 공개키로 1차 메세지를 암호화하고 자신의 비밀키로 2차 암호화해서 보낸후, 수신자는 먼저 상대의 공개키로 복호화한 후 자신의 비밀키

로 2차 복호화를 하는 방식이 있고 여기에 one way hash function을 결합해서 보다 간결하고 강화된 서명 스킴을 만들 수 있다.

#### ① 식별

송신자(사용자/클라이언트) A는 수신자(시스템/서버) B에게 자신이 A임을 설명할 수 있으나 임의의 제 3자 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 틀 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. 멀티 로그 인 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 KERBEROS/DCE/SESAME등을 이용하여 네트워크 접속 통제를 하는 양방향 식별 혹은 인증 방식이 있다.

#### ① 암호

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, 메시지 암호화/복호화시 사용하는 방식이고(DES:Data Encryption Standard), 공개키 방식은 송/수신자간에 별도의 암호화/복호화 키를 소유하고 메시지

전송시만 서로간에 공통키를 소유하여 송/수신하거나 공개된 암호화 키로 암호화하여 복호화 키를 갖고 있는 사람 많이 복호화 할 수 있도록 하는 형태(RSA:Rivest, Shamir, and Adelman)가 있다.

#### ① 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.

#### ① 자동복제 관리기술

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

#### ① 프라이버시 보호기술

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

#### ① 정보 중복 및 분산 기술(유용성/신뢰성)

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

#### ① 시스템 이중화(유용성/신뢰성)

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

## 6. 안전성 대책 방향

초고속정보통신기반하에서 수립되어야 할 안전성 대책 방향은 먼저 응용서비스별 안전성 요구사항을 파악하고, 안전성 기본 원칙과 정보와 시스템에 대한 기본원칙을 정의하여 안전성 프레임워크를 설정하는 것이다. 그리고 안전성 프레임워크를 바탕으로 서로간의 역할을 정립하고 법적/제도적 측면의 통제와 시행에 대한 준비와 기술적/관리적 측면의 준비를 하는 것이다. 본 소절에서는 시큐리티 프레임워크를 확립하기 위한 구체적인 안전성 대책 방향을 살펴 본다.

### 6.1 Coordinating기능 정의

서로간의 역할 정립을 정의하는 Coordinating기능은 초고속정보통신기반하에서 다음과 같은 사항이 고려되어야 한다.

- ① 국가 경제/보안 측면
- ① 윤리/교육적 측면
- ① 비상 준비/대응 측면
- ① 품질 보증 측면

### 6.2 법적/제도적 통제와 시행 준비

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

- ① 초고속정보통신기반하에서 관련된 종합적인 법적/제도적 규제와 시행 측면 제시 (전기통신법/컴퓨터프로그램보호법/통신비밀보호법/저작권법/기타 전기/통신/방송/유선/무선 관련 법/제도)
- ① 민법 측면
- ① 형법 측면
- ① 국제 협력 측면

### 6.3 기술적/관리적 대책 준비

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

#### ① 시스템 보호 측면

- 시스템 접근제어(패스워드/개인식별/인증/감사)
- 게이트웨이 보호(Firewall)
- 시스템/네트워크 보호(신뢰성/안정성/이중화)

#### ① 정보 보호 측면

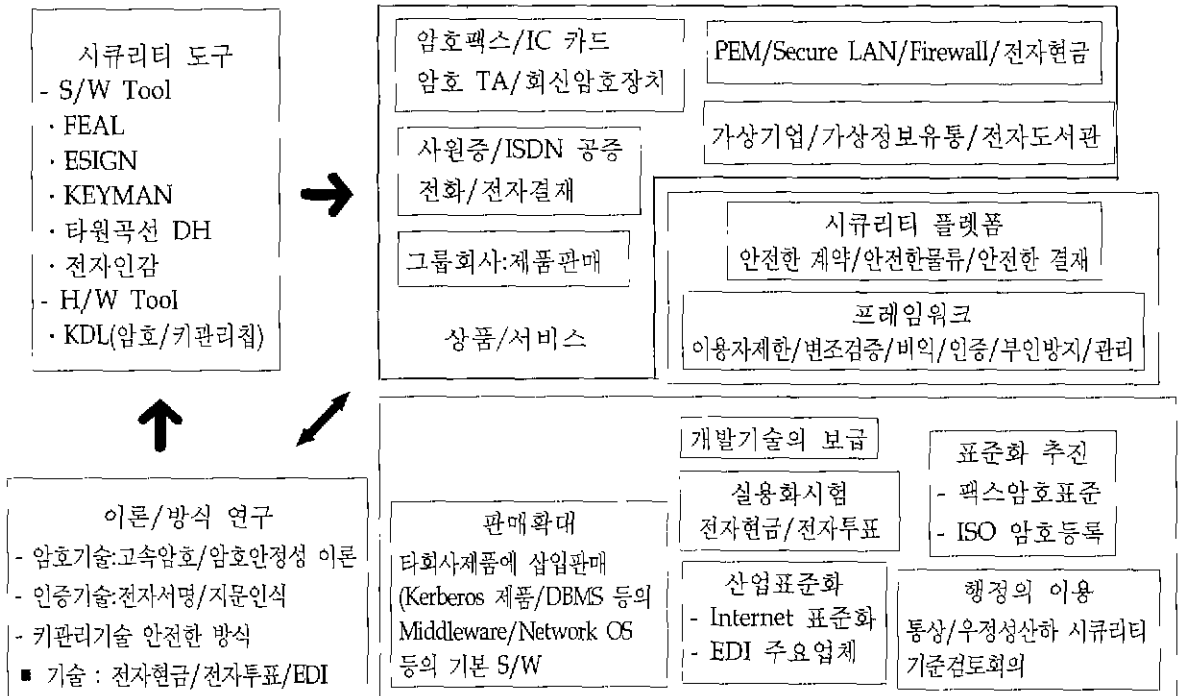
- 정보 접근제어(패스워드/개인식별/인증/암호화/감사/분산/백업)
- 복사에 대한 보호(자동복제관리시스템)

시스템과 정보의 기술적 보호에서는 앞에서 언급한 보안서비스가 다중 형태로 적용되도록 고려해 할 것이다. (그림 3)은 기술적 차원의 시큐리티 대책 흐름 [5]의 일본 예이다.

## 7. Secure NII를 위한 정부 역할

앞에서 제시한 안전성 대책 방향을 종합적이고 구체적으로 진행하고 초고속정보통신기반 하에서 요구되는 안전성 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 NII의 민간활동을 증진하는 시설 지원자 혹은 촉진자로서 역할, 대중 이익 및 일반 복지 보호자로서 역할, 중요 연구분야에 대한 자금지원과



(그림 3) 시큐리티 기술적 대책 흐름 (일본 NTT)

민간분야에 필요한 기술 개발 지원자로서 역할, 그리고 마지막으로 NII 이용자로서 역할과 정부 정보의 보호 및 책임이다. 이와같은 정부의 역할을 추진하고 Secure NII를 실현하기 위해서는 각 역할에 따른 필요한 준비가 있어야 하겠다.

- NII의 민간활동을 증진하는 시설 지원자 혹은 촉진자로서 역할
  - 시큐리티 위협요인 증대 인식과 이의 해결책의 필요성 인식 고취
  - 시큐리티에 대한 이용자 요구사항 파악을 바탕으로 정보 및 시스템에 대한 시큐리티 기본 원칙 수립
  - NII에 유용한 보안 장비와 기술의 개발 보급
  - 신뢰성있고 안전한 고품질 보안 장비/보안기술의 민간 개발 유도
- 대중 이익 및 일반 복지 보호자로서 역할
  - NII에서의 적절한 비상 대처 능력 준비

- NII에 맞는 법적/제도적 통제
  - NII환경에 맞는 각종 법적 준비
  - NII/GII 환경에 따른 국제적 대처 준비
  - 중요 연구 분야에 대한 자금지원과 민간분야에 필요한 기술 개발 지원자로서 역할
  - NII 이용자로서 역할과 정부 정보의 보호 및 책임
    - 정부정보에 대한 적절한 관리과정 수립과 보안 요구사항 수행
    - 정부의 보안 비상 능력 준비
    - 보안기술/장비의 신뢰성/안전성
    - 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.



## 8. 결 론

초고속정보통신기반의 발전을 좌우할 시큐리티는 그 대책을 수립하는데 있어 먼저 이용자와 서비스 제공자의 안전성 요구사항을 파악하는 것이 가장 중요하다. 이용자와 서비스 제공자의 안전성 요구사항을 파악하는데 있어서는 NII상에서 가장 많이 이용될 전자사업 서비스(게임/오락/소프트웨어/기타 컴퓨터 서비스등)에 대한 사항, 금융/재정/보험 관련 서비스에 대한 사항, 의료/건강/보건에 관련된 사항, 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 NII시큐리티에 대한 기본원칙 수립과 이를 바탕으로 시큐리티 대책의 기본요소인 법/제도/기술/관리 사항이 종합적으로 표현된 시큐리티 프레임워크와 역할정립은 초고속정보통신기반하에서 안전성 대책이 진행되어야 할 방향이라 하겠다. 특히, 초고속정보통신기반하에서 더욱 다양해지는 안전성 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.

### 참고문헌

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

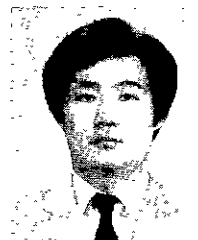
[2] 김광조, 보안시스템의 최근 기술 동향, NET-SEC-KR 96, 1996.5  
 [3] 박정현, 초고속정보통신기반하에서 안전성 요구사항, AIN96, 1996  
 [4] Sharnir, Identity-Based Cryptosystems and Signature Schemes, Proc. of Crypto84, 1984  
 [5] Gary S. Morris, Computer Security and the Law, GSM Associates, 1996  
 [6] Timothy D Schoechle, Privacy on the Information Superhighway, CyberLYNX Gateway Corporation, 1996  
 [7] Rick Nevins, AMP, Incorporated Network Security, Global IT Infrastructure, 1996



**박 정 현**

1982년 숭실대학교 전자공학과 졸업 (학사)  
 1985년 숭실대학교 대학원 전자공학과 졸업 (공업석사)  
 1997년 충북대학교 대학원 전자계산학과 졸업 (공학박사)

1982년-현재 한국전자통신연구원 초고속정보통신연구본부 (선임연구원)  
 관심분야 : 암호이론 및 응용, 키분배 및 암호화 프로토콜, 위성 방송/통신



**이 상 호**

1976년 숭실대학교 전자계산학과 졸업 (학사)  
 1981년 숭실대학교 대학원 전자계산학과 졸업 (공업석사)  
 1989년 숭실대학교 대학원 전자계산학과 졸업 (공학박사)

1981년-현재 충북대학교 컴퓨터과학과 교수  
 1989년-1990년 호주 텔레콤 방문 연구원  
 1992년-1993년 캐나다 UBC 전자계산학과 방문 연구원  
 1994년-현재 충북대학교 전자계산소장  
 관심분야 : 프로토콜 공학, 컴퓨터 통신, 암호학, 시뮬레이션