□ 기술해설 □

# 초고속 정보화를 위한 보안 소프트웨어 기술개발 계획

아주대학교 최덕규* · 윤기송**

목 차



## 1. 서 론

최근 정보산업의 급격한 발전에 따라 정보산업 육성을 위한 대규모 전산망 계획이 국가적 차원에서 진행되고 있다. 우리나라의 초고속 정보통신망 계획을 비롯하여 미국의 NII(National Information Infrastructure), 유럽의 Big Bang, 일본의 신사회자본, 싱가폴의 TI2000 등 초고속 정보통신망 계획을 통하여 국민 생활 향상 및 국가경쟁력 강화에 힘쓰고 있다. 또한 각국의 전산망은 서로 연동하여 경제, 과학, 기술 등 모든 분야에서 이미 정보의 국제화 시대는 시작되었다. 전산망 관련기술의 발전, 컴퓨터 및 전산망 사용자의 급격한 증가, 전산망 규모의 성장, VOD, 가상현실 등과 같은 다양하고 새로운 전산망 서비스의 요구 등에 따라 앞으로 전산망의 발전은 더욱더 빠른 속도로 진행될 것으로 예상된다.

이러한 전세계에 걸친 다양한 분야에 다양한 서비스가 생겨나면서 주요한 전산자원 즉 하드웨어, 소프트웨어, 기밀을 요하는 국가정보, 산업기술정보, 개인정보에 관련된 데이타베이스를 외부로부터의 침입, 변조, 도용 또는 도난을 방지하고 추적하는 이른바 전산망 보안이 중요한 컴퓨터의 한 분야로 나타나고 있다. 특히 우리나라의 초고속 정보통신망의 구축에는 2015년까지 약 45조원에 달하는 엄청난 규모의 투자를 필요로 하는 초대형 과제라고 할 수 있다. 만약 초고속 망이 완료된 후 주요 데이타의 도용, 변조, 파괴 또는 주요시스템의 불법사용 등 전산망 보안이 보장되지 않을 경우 초고속전산망의 사용은 극히 제한된 범위로 축소될 수 밖에 없다. 따라서 투자와 HCI, 정보처리, 표준화 등 타 전산망 기술분야의 효용극대화를 위하여 또한 전산망을 통한 새로운 산업을 육성하기 위하여 전산망 보안의 확보는 필수적이라 하겠다.

최근 인터네트와 연동하는 국내기관이 대학, 연구소, 국가기관, 일반기업체 등 약 200여 기관으로 늘어나면서 전산망의 사용이 확산되어가고 있는 반면 1994년 11월 원자력 연구소 해킹

*종신회원
**정회원

사건을 비롯한 일련의 전산망 보안 사고는 정보통신 보안기술의 중요성을 보여주었다.

### 1.1 보안 기술의 특성

초고속 정보통신 보안기술은 크게 암호화, 시스템 보안, 전산망 보안의 세가지 기술로 분류할 수 있으며 다음과 같은 특성을 가지고 있다.

첫째, 정보통신 보안기술은 지속적으로 update 되어야 한다. 전산망 기술환경은 항상 변화하고 있다. 새로운 데이타 전송방식, 전송 매체, NIS, NFS, Mosaic 등과 같은 새로운 서비스가 나타남에 따라 전산망 침해기술도 다양하게 나타나므로 전산망 보안 기술도 따라서 발전해야 한다.

둘째, 정보통신 보안기술은 불특정사용자를 대상으로 한다. 각 분야의 전산망이 국제적으로 상호 연동하면서 전산망 사용자의 수는 급증하게 되며 국제망과 연동하고 있는 전산망은 전세계로부터 수천만명 이상의 불특정 사용자로부터의 해킹 위험성은 항상 존재한다.

셋째, 암호화기술은 국내외 타전산망과의 호환성이 필요하다. 전산망을 통하여 암호화된 데이타를 주고 받을 때 표준화된 암호방식 및 키 관리방식에 따른다.

넷째, 정보통신 보안기술은 타전산망과의 공조체제를 통하여 완성된다. 전산망 보안사고는 초고속 전산망 기술의 발전에 따라 다른 전산망을 다단계 경유하여 발생하는 것이 일반적 현상이다. 따라서 국내외 전산망과의 기술적, 관리적 협력체제가 필요하다.

다섯째, 완벽한 정보통신망의 보안이 어렵다. 컴퓨터의 성능향상으로 암호화된 데이타의 복호화의 가능성이 있고 암호화기법은 비밀번호를 사용하고 비밀번호는 항상 노출의 가능성이 있으며 응용소프트웨어의 보안성검증의 어려움이 있다.

여섯째, 정보통신망 기술은 국가보안기관과의 협조체제가 필요하다. 정보통신 보안기술은 국가안보와 관련이 있으므로 국가보안기관과의 긴밀한 협조체제위에서 진행되어야 한다. 또한 국제적 해킹에 대비한 국가간 협조체제와 국가보안을 위한 특정분야에서의 강제규정을 위하여 국가기관과의 긴밀한 협조체제가 필요하다.

### 1.2 보안 기술의 중요성

전산망 보안 기술의 중요성은 다음과 같다.

첫째, 응용서비스 측면에서 기밀성 확보를 통하여 국방, 외교, 안보 등 국가기밀정보의 안전한 보호전달 체계를 갖추어 신속한 국가정보 수집, 전파, 저장하고 무결성 검증기능을 통하여 정부기관과 관련한 전자 민원, 전자입찰 등 전자문서의 변조방지하여 전자문서 사용의 일반화를 도모하고 국가간 기업간 전자 결재시스템을 통하여 무역자동화를 조기에 정착시킨다. 기업체의 주요 기술정보를 안전하게 저장하고 EDI를 통하여 대용량의 정보를 신속 안전하게 처리하고 개인의 의료 및 신용 정보 등 개인의 사생활정보 보호한다. 또한 컴퓨터 범죄 방지기능을 통하여 컴퓨터 범죄를 처리하고 전산망 보안관리를 통하여 컴퓨터 범죄 증거 확보하며, 주요 전산자원(시스템, 소프트웨어, 데이타베이스 등)을 보호하고 해킹 방지 및 해커 추적을 통하여 전산망 사용자의 보안 의식을 고취시킨다.

둘째, 기술환경 발전 측면에서 전산망 기술발전에 따른 전산망 침입 기술의 발전대비, 다양한 전산망 서비스 출현에 따른 다양한 보안사고 대비, 전산망간의 연동에 따른 보안사고의 확대방지, 다양한 전산망 프로토콜의 출현에 따른 보안 기술 대비, 보안 사고의 신속한 대응책 요구 및 불특정 다수의 전산망 사용자 관리를 위한 보안 기술이 필요하다.

셋째, 전산망 보안 기술의 파급효과로는 전산망을 통한 정보전달체계에 대한 신뢰성을 높혀 전산망 사용의 안정화를 도모하여 초고속 정보화 사회의 조기 정착에 기여한다.

### 1.3 국책 연구 개발 추진의 필요성

국책연구개발 추진의 필요성으로는 다음과 같다.

첫째, 공통 핵심 보안기술의 개발 및 보급은 국가안보와 관련있는 중요한 기술이므로 국가보안 기관과의 협력이 필요하다.

둘째, 정부기관에서 발행하는 전자문서의 암호화, 무결성 검증, 정부부처간 전자 결재, 국가와 국가, 정부와 산업체, 정부와 개인간의 전자문서 교환 등 정부관련 전자정보에 대하여 기밀성을 유지하고 공신력을 확보하여야 한다.

셋째, 산·학·연·관 공동노력을 통하여 보안 기술을 향상시켜야 하며 24시간 전산망 보안 비상체제의 운영, 국가기간전산망 및 상용전산망의 보안관련 공조체제 유지 및 국가 차원의 전산망 보안의식을 고취시켜야 한다.

넷째, 초고속 전산망 보안 표준제정을 통하여 소프트웨어 개발 생산성 향상 및 국제표준과의 호환성을 유지하며 국제적 전산망 보안 사고 발생시 신속한 국가간 공조체제를 유지하여야 한다.

다섯째, multi-media, 컴퓨터 게임분야 등과는 달리 자발적인 민간의 기술개발 참여유도의 어려움을 고려하여야 한다.

## 2. 기술 동향

### 2.1 해외 기술 동향

암호화 기술의 동향은 ISO/IEC/JTC1와 CCITT의 보안 기술 표준화 활동을 중심으로 블럭암호 운영모드, 실체인증, 데이타 무결성, 부인 봉쇄, 전자서명, 전자서명과 인증기법을 위한 해쉬함수, 정보보안 평가기준, 영지식을 이용한 보안 기법, 키관리기법 등에 관련된 기술에 대한 활동을 하고 있다. 또한 Internet에서는 IETF(Internet Engineering Task Force) Security Area를 중심으로 Security Guide 제작 및 규격화된 보안 기능방식 연구, 응용계층에서의 firewall 지원방식 연구, 인터네트의 망 서비스에 강화된 인증 기능 보완 연구, IPSO(IP Security Option)의 미국외 국가 및 일반 사용을 위한 연구, 데이타 비밀등급 분류, DNS 데이타 보호, 데이타보호를 위한 전자서명 기법 연구, 네트워크계층에서의 보안 방식 연구, Network Access Server의 기능 및 서비스 연구, 인터네트의 전자우편기능에 보안 기능추가, 일회용 비밀번호 연구 등의 활동이 있다.

시스템 보안 분야의 활동은 주로 미국을 중심으로 이루어지고 있다. 미국 국방성에서는 컴퓨터 시스템이 갖추어야 할 보안 장치를 명문화한 Trusted Computer Systems Evaluation Criteria (TCSEC 또는 Orange Book)이라 불리우는 기준을 1985년에 설정하였으며 국가 컴퓨터 보안국(National Computer Security Center)의 주관으로 Trusted Products Evaluation Program (TPEP)을 운영하고 있다. TPEP는 TCSEC에 명시된 등급 및 각 등급에서 요구하는 보안장치의 요구사항을 중립적인 위치에 있는 전산전문 평가자들이 운영체제, 데이타베이스, 전산망 구성요소들을 보안 측면에서 검사한다. 미국에서는 현재 TCSEC를 개정하여 Commom Criteria라고 불리우는 개정 보안 기준을 마련 중이다. 이는 유럽이나 카나다 등의 보안기준과의 호환성을 유지하게 된다.

미국의 경우 전산망 보안문제에 효과적으로 대응하기 위해 미국방성의 후원으로 CERT(Computer Emergency Response Team)을 운영하고 있으며, Stanford Reseach Institute International 같은 연구소에서는 미해군의 후원으로 컴퓨터망에 있을지도 모르는 무단 침입자를 실시간에 감지하기 위한 전문가 시스템을 개발하고 있다. Intrusion Detection Expert System(IDES)라 불리우는 이 시스템은 한 개 또는 여러 개의 컴퓨터 시스템의 사용자를 감시한다. 이 시스템은 각 사용자의 전형적인 사용양식을 저장하고 기록하여 이용할 뿐 아니라 사용자의 이용양식의 변화의 학습기능을 보유하고 있다. 또한 이미 알려져있는 시스템의 보안 취약점과 그에 따른 침입경로를 예측하여 감시할 수 있는 기능을 갖추고 있다.

### 2.2 국내 기술 개발 동향

○암호 알고리듬 개발 및 장비개발
－ETRI 부호기술부
－국방과학연구소
－국방체계연구소
－국방대학원, 포항공대
○보안 서비스 개발

- 암호 관련 기술 적용
- 충남대 : 키관리 메카니즘
- 포항공대 : 전자서명, Smart Card 등
- 기타 국방대학원, 아주대

○ 전산망 보안－OSI 보안, LAN 보안

- ETRI
- ETRI PEC : OSI Transport 계층의 보안 프로토콜 개발중
- 광운대학, 경북대학 : IEEE SILS 연구
- 아주대학 : OSI 응용 계층의 공통 보안 서비스 모델
- SERI : OSI 수송계층 보안연구, OSI 응용계층 공통 보안 서비스

○ 전산망 보안－응용 서비스 보안

- 아주대학 : MHS 보안
- 성균관대 : EDI 보안
- 국방대학원 : MHS를 위한 키관리
- SERI : Internet Mail의 보안

○ 시스템 보안

- ETRI : PC 보안 패키지 개발중
- 숭실대 : IDES(Intrusion Detection Expert System) 연구
- 한국전산원 : 주전산기 보안 패키지 구현
- 전남대 : 보안 모델 연구

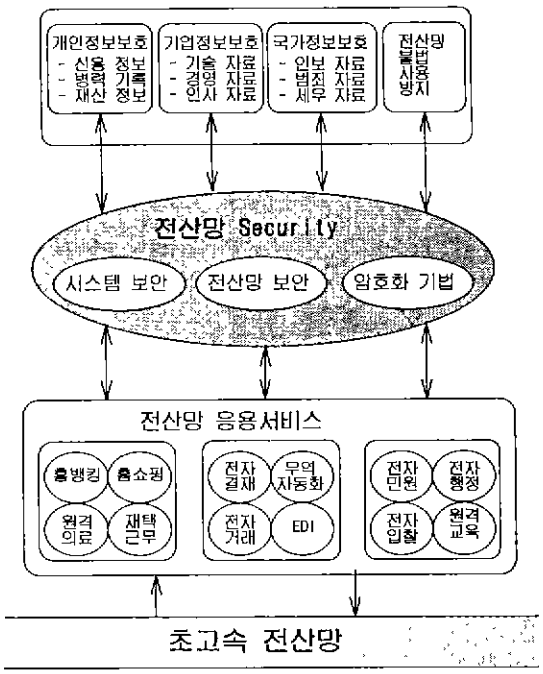


그림 1 최종개발 목표

## 3. 연구개발 목표

### 3.1 최종개발 목표

본 연구에서는 초고속 정보통신 환경에서 주요 전산자원 및 국가, 기업, 개인정보를 보호하고 국가보안기관에서 인증받을 수 있는 시스템보안, 전산망 보안 암호화기법을 통한 소프트웨어적 보안기술개발을 최종 개발 목표로 삼고 있다(그림 1).

### 3.2 단계별 연구 목표

위의 최종목표 달성을 위하여 기술환경의 변화에 따라 2015년까지의 단계별 목표설정이 필요하다. 1단계(1995～1997)에서는 초고속 시범 전산망에서의 보안 기술의 시범적용 및 보안 특성별 기반기술을 개발하고, 2단계(1998～2002)에서는 고속 전산망 환경에서의 보안 기반기술의 안정화 및 응용기술을 개발한다. 또한 3단계(2003～2007)에서는 국제적 초고속 대용량 환경에서의 통합 보안 전산망 기술을 개발하고, 4단계(2008～)에서는 첨단 초고속 환경에서의 지능형 전산망 보안 기술을 개발한다(그림 2).

## 4. 기술 체계

초고속 전산망 보안기술은 크게 시스템 보안,

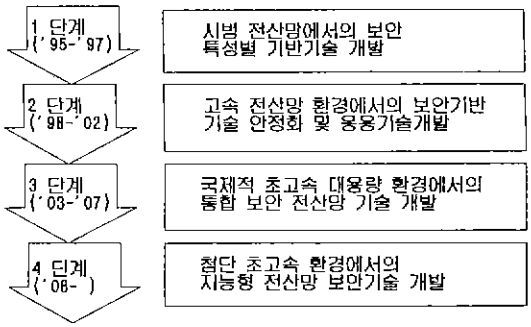


그림 2 단계별 연구 목표

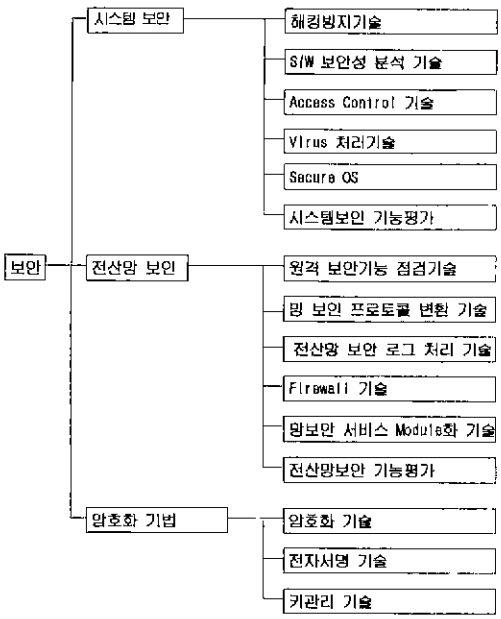


**그림 3 초고속 전산망 보안기술의 체계**

전산망 보안, 암호화의 세 분야로 분류한다(그림 3).

### 4.1 시스템 보안 기술

－해킹방지

해킹 가능성을 사전에 예방하기 위하여 하드웨어, 소프트웨어의 보안취약성 진단, 사용자들의 시스템 사용 관리, 모니터링을 통하여 사전에 시스템 침입을 예방하고, 다양한 경로를 통한 해킹을 감지하고 해킹형태를 분석한다. 또한 해커의 위치를 실시간 추적하고 보안 사고를 복구한다.

－소프트웨어 보안성 분석

전산망에서 제공되는 모든 서비스는 시스템 또는 응용 소프트웨어를 통해 제공되고 있으며 일반적으로 해킹은 대부분 이러한 소프트웨어의 보안취약성을 통하여 행해지고 있다. 전산망 운영에 사용되는 소프트웨어의 보안 취약성을 찾아낸다.

－접근제어 (access control)

다양한 전산자원 (하드웨어, 소프트웨어, 데이타베이스)의 사용을 인증받은 사람에 한해서 사용하게 하여 불특정 다수의 사용자로부터 주요 전산자원을 보호한다.

－바이러스 처리

주요 데이타 및 소프트웨어를 파괴하는 바이러스를 비롯한 worm, 박테리아 등 다양한 형태의 악성 프로그램을 제거시킨다. 이러한 악성 프로그램의 패턴을 인식하여 궁극적으로 인체의 항체 자동생성과 같은 시스템을 개발한다.

－Secure OS 개발

사용자 관리, 비밀번호 관리, 화일시스템의 변조방지 및 검증, 망 서비스 접근제어, 관리자 권한분산 등의 기능을 OS에 통합한다.

－시스템 보안기능 평가

시스템 보안 평가의 기준을 설정하고 시스템 보안기능의 평가를 자동화한다.

### 4.2 전산망 보안 기술

－원격 보안 기능 점검

해킹예방, 탐지, 추적, 복원, 소프트웨어 보안성 분석, 접근제어, 바이러스 처리기술 등 한 시스템 내부에서의 이루어지는 기술을 보안센타와 같은 원격지에서 전산망을 통하여 동시에 많은 시스템의 보안 관리를 가능하게 한다.

－전산망 보안 프로토콜 변환

상이한 프로토콜을 사용하는 전산망이 게이트웨이를 통하여 상호연동시 암호화, 키관리, 사용자정보 등 보안정보의 상이성에 대한 투명성을 제공한다.

－전산망 보안로그 분산처리

전산망 보안처리를 위하여 전산망내 시스템들에 분산되어 있는 대용량 보안기록을 신속한 처리를 통하여 필요한 전산망 보안 정보를 처리한다.

－방화벽(firewall) 기술

특정한 전산망을 외부 전산망으로부터 격리하여 특정 전산망의 내부 정보를 보호하고 외부에서 들어오는 정보와 사용자를 선별하여 전산망의 보안성을 향상시킨다. 또한 전산망의 일부를 보안환경에 따라 전산망의 범위를 재조정한다.

－전산망 보안 서비스 module화

전산망 응용 서비스에 필요한 암호화, 인증,

키관리 등 공통 보안기능을 분리하여 응용서비스가 공통적으로 사용하고 응용서비스의 개발시 보안 관련기능은 공통 보안 서비스 module을 사용하게 한다.

－전산망 보안 기능 평가

전산망 보안평가 기준을 설정하고 전산망 보안기능의 평가를 자동화한다.

### 4.3 암호화 기법

－암호화

초고속 전산망에서 응용서비스를 통하여 전달되는 대용량 데이타의 암호화를 위한 새로운 암호화 기법을 개발하고 실시간 암호화 처리를 수행한다.

－전자서명

초고속 전산망에서 응용서비스를 통하여 전달되는 대용량 데이타의 변조방지를 위한 무결성 검증 방식으로 새로운 전자서명 기법을 개발하고 실시간으로 처리한다.

－키관리

초고속 전산망 환경에서의 응용서비스별로 보안 기능에 필요한 데이타의 암호화와 전자서명에 필요한 키의 분배 및 관리를 호율적으로 하기 위한 메카니즘을 연구개발한다.

## 5. 연구개발 추진 계획

초고속 정보통신망 보안기술 연구개발은 5장에서 제시한 기술들을 통합·분류하여 과제를 도출하고 초고속망 보안기술 개발센타를 중심으로 연구소, 대학, 기업체와 연계하여 추진한다. 모든 보안기술을 기초연구부터 시작하는 방식을 지양하고 기술 분야별로 현재의 국내외 기술을 도입, 전수 또는 공동개발 등을 통하여 현재의 기술수준을 기준으로 연구개발을 시작한다. 또한 실제 망에서 사용될 수 있는 기술을 개발하기 위하여 국가기간전산망 및 상용전산망의 운영과 유기적인 정보협력체제를 구축한다. CERT(Computer Emergency Response Team)와 같은 국내외 보안기관들과 기술협력관계를 유지하며 상호 호환성을 위하여 국내외 표준활동에 주도적으로 참여하고 국가 정보기관과 유기적인 협력관계를 통하여 국가 전체차원에서 연구개발을 수행해 갈 수 있도록 한다. 또한 1단계의 시범전산망에서의 보안기술을 개발하고 2, 3, 4단계의 단계별 기술개발을 통하여 최종적으로 초고속 정보통신망에서의 보안기술을 완성한다.

### 5.1 연구과제 도출 기준

위에서 언급한 연구개발 추진 계획에 따라 연구과제를 도출하기 위한 기준을 다음과 같이 정하였다.

◦ 초고속 정보통신망 사용의 신뢰성을 높여 정보화 사회의 조기안정화에 필수적인 과제

◦ 국가차원에서 반드시 수행되어야 하는 과제

◦ 1 단계 완료시 국가망 또는 상용망에서 실제 사용가능하고 지속적으로 기능 향상이 필요한 과제

◦ 연구의 결과를 통하여 국제적 전산망 보안사고 대비를 위해 국제적 공조체제 유지에 필요한 과제

◦ 보안분야의 특성상 우리나라 고유의 기술개발이 필요한 과제

◦ 경제적, 사회적, 기술적 파급효과가 크고 전산망 보안기술의 표준이 될 수 있는 과제

◦ 국내외 연구 활동과 연계하여 기초연구에서 시작하거나 중복개발이 아닌 과제

◦ 관련 기술체계도와 연구과제 상호간의 연계를 고려하여 도출한 과제

◦ 연구개발을 위한 인적, 물적자원 등 resource를 고려하여 도출한 과제

◦ 개발 내용의 명세화가 가능한 과제

### 5.2 연구과제 분류

이러한 연구과제를 분류하면 그림 4와 같다.

### 5.3 연구과제 체계도

연구과제 체계도는 그림 5에 나타내었다.

### 5.4 연구개발 수행 체계

| 대과제명 | 초고속 정보통신망 보안 S/W 개발 |
|---|---|

| 소과제명 | 내 용 |
|---|---|
| 전산망불법사용방지 시스템개발 | ○ 전산망 및 시스템 보안 전담 기능<br>○ 해킹 탐지 및 실시간 추적 기능<br>○ VIRUS 방지도구 개발 |
| 전산망공통 보안기능지원 시스템개발 | ○ 전산망 응용 서비스공통 보안 라이브러리 개발<br>○ 보안 관리용 지원 도구 개발<br>○ 전산망 표준 데이타 보안 모델 개발 |
| Secure OS 개발 | ▫ Password , 최종 보안관리<br>○ 접근제어<br>○ Auditing<br>○ 관리자 권한 분산 |
| 보안기능 평가시스템 개발 | ○ 시스템 및 전산망보안 평가기준설정<br>○ 시스템 및 전산망 보안 평가 지원툴 |
| 암호화 키관 | ○ 암호화<br>○ 인증<br>○ 전자서명<br>○ 키관리 |

그림 4 연구과제 분류

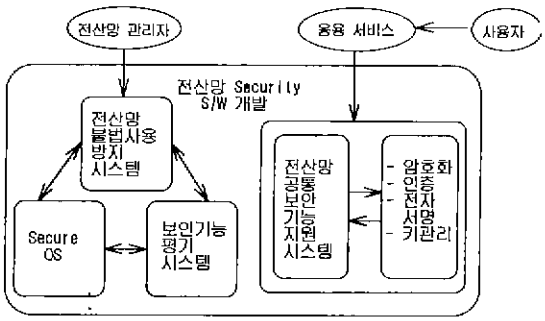


그림 5 연구과제 체계도

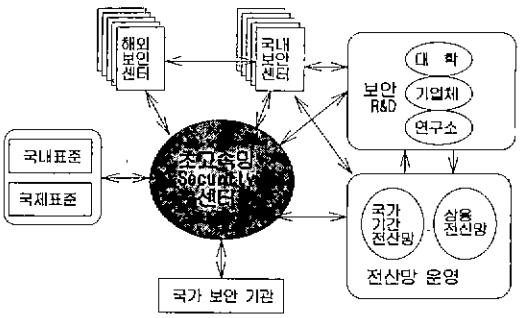


그림 6 연구개발 수행 체계

연구개발 수행체계는 그림 6에 나타내었다.

## 6. 결 론

### 6.1 기대되는 연구결과

초고속 정보통신망 보안 소프트웨어 개발을 통하여 기대되는 기술적 연구 결과로는 전산망 표준 데이타보안 모델 제시, 보안 기능의 효율성 향상, 공통 보안기능의 분리로 응용서비스 개발의 용이, 전산망 보안기능의 투명성 제공 등이 있다. 최종적으로 주요 전산자원의 보호, 전산망 보안 사고피해의 최소화, 전산망 보안 사고에 대한 대응 능력 향상, 초고속 정보통신망의 신뢰성 증가, 전산망 불법사용 기도의 사전 억제, 정보화사회의 조기 정착에의 기여 등의 결과를 예견한다.

### 6.2 연구결과 활용방안

초고속 정보통신망 보안 소프트웨어 연구결과의 활용방안으로는, 국가기간 전산망 및 일반 상용망에 보급 활용, 국내외 전산망 보안 기술 표준으로 활용, 국내외 보안 공조체제, 초고속 정보 통신망의 안정적 사용의 핵심기술, 컴퓨터 범죄 증거확보, 전산망 불법 침입 데이타베이스 구축 등으로 활용한다.

## 참고문헌

[1] Proceedings of Tenth Annual Computer Security Applications Conference Dec. 5-9, 1994.

[2] "Kerberos: An Authentication Service for Computer Networks" B. Clifford and Theodore Ts'o IEEE Communications, Sep. 1994.

[3] "Access Control: Principles and Practice" RaviS. Sandhu and Pierangela Samarati IEEE Communications, Sep. 1994.

[4] "Network Fire Walls" Steven M Bellvin and William R. Cheswick, IEEE Communications. Sep. 1994.

[5] The Canadian Trusted Computer Product Evaluation Criteria Version 3.0 January 1993.

[6] Achieving Security in an Internet Environment, USENIX Winter 1994 Conference, Jan. 17-21, 1994.

[7] The Kerberos Network AUthentication Service (RFC 1510) J. Kohl, Digital Equipmemt Corporation, Sep. 1993.

[8] Generic Security Service API(RFC 1509) J Wray, Digital Equipmemt Corporation, SEp. 1993.

[9] Privacy Enhanced Mail (RFC 1421-1424) Feb. 1993.
[10] Telnet Authentication : Kerberos Version 4, D. Borman, Editor, Cray Research, Inc.
[11] Final Evaluation Report American Telephone And Telegragh System V/ MLS Release 1.2.0 Running On UNIX System V Release 3.1.1 National Computer Security Center, Sep. 28, 1990.
[12] Final Evaluation Report Trusted Information Systems, Inc. National Computer Security Center, Jan. 22, 1991.
[13] 김동규 외 "정보통신 네트워크 안전체제의 신분확인 및 액세스 제어 연구", 한국 전자통신연구소 최종 보고서, 1990. 5.
[14] 박형선 외 "네트워크 자원에 대한 액세스 제어 시스템", 한국 정보보호학회 종합학술발표회 논문집, 1994. 11. 19.
[15] 신동익 "위험 관리 체계연구", 한국 정보보호학회 종합학술발표회 논문집, 1994, 11. 19.
[16] 이필중 외 "해외의 보안 위험 분석 방법론 현황 및 분석" 한국 정보보호학회 종합학술발표회 논문집, 1994. 11. 19.
[17] "국가기간 전산망 안전보장 중장기계획", 한국전산원, 1994, 12.
[18] "인터네트 보안 지침서" 시스템공학연구소 연구전산망 개발실, 1994. 8.
[20] 문상재 "컴퓨터 범죄방지를 위한 정보통신망의 보호방안에 관한연구", 정보통신보호학회지, 1994, 6.
[21] 이필중 "ISO/IEC JTC1/SC27의 국제 표준소개", 정보통신보호학회, 1994. 8.

**최 덕 규**

1966 서울대학교 원자력공학과 졸업
1984 Wright State University, 전산학 석사
1989 University of Massachusetts, Lowell, 전산학 박사
1968 ~1970 KIST 연구원
1971 ~1975 CDK S.E.
1976 ~1991 국방과학연구소 책임연구원
1992 ~현재 고등기술연구원 연구위원 아주대학교 부교수
관심 분야 : 데이타 통신/컴퓨터네트워크, 네트워크 표준화 근거리통신망 프로토콜 및 Performance

**윤 기 송**

1976 ~1983 부산대학교 졸업
1986 ~1988 City University of New York 전산학 석사
1989 ~1993 City University of New York 전산학 박사
1993 ~현재 시스템공학연구소 선임연구원
관심 분야 : 데이타 통신/컴퓨터네트워크, Network Security, 병렬처리