□ 기술해설 □

국내·외 정보보호관련 연구 동향

한국정보보호센터 이철원·홍기웅*·김학범**
이경구·오경희**·심주걸

1. 서 론

오늘날의 정보는 더이상 사람이나 종이 또는 문서에 의해서만 저장 및 처리되는 것이 아니라 정보시스템에 의하여 저장 전송 처리되고 있으며 전자문서에 대한 유효성 및 적법성도 법 제도적인 측면에서 고려되어가고 있는 실정이다.

또한, 선진 각국에서 뿐만 아니라 국내에서도 국민 개개인에 대한 각종 공공서비스의 질적 향상 및 효율적인 촉진을 위하여 각종의 정보시스템을 도입 운영함은 물론 정보화 촉진을 위하여 범정부 차원의 전산망 기술 보급 및 지원 체계를 구축해 나아가고 있다.

이러한 정보화 촉진을 보다 효율적, 체계적, 안정적으로 추진해 나가기 위해서는 컴퓨터 범죄나 해킹과 같은 위협으로부터 각종 전산망 및 정보시스템이 안전하게 보호되어야 하며 이를 위한 대책 수립이 체계적으로 이루어져야 한다.

이를 위하여 선진 각국은 정보보호를 위한 각종 정책 및 기술의 연구 개발을 통하여 효율적인 정보보호체계를 구축해 나가고 있다. 또한 정보보호 정책의 체계적인 실현 및 기술개발을 위하여 국가적 차원의 정보보호 관련 기관들을 설립 운영하고 있다.

본 고에서는 국내외 정보보호 관련 정책, 기술 동향 및 표준화에 대한 조사 분석을 제시하고자 한다.

*종신회원
**정 회 원

2. 국외 정보보호 관련 정책

2.1 미국의 정보보호 관련 정책

미국은 정보보호 분야에 있어서 선도적이라 할 수 있을 정도로 1960년대부터 정보보호 관련 기술에 대한 연구 개발을 시작해 왔다. 1984년 이전까지는 주로 국가 비밀에 관련된 사항은 국방부가 관장해 왔고 국가 비밀이 아닌 사항은 상무부의 책임이었다. 국가 보안의 경우 국방부와 중앙정보부가 보안 정책을 개발하는 임무를 수행하였고, NSA는 표준화, 연구개발, 평가 및 기술 자문 등의 임무를 수행하였다. 민간 부문에 대한 보안의 경우 행정관리예산청이 정책 개발을 주도하였고 표준화 및 기술 자문에 관한 임무는 NIST의 전신인 미국립표준국(National Bureau of Standard : NBS)이 맡아 수행하였다. 1985년 이후에는 NSDD-145에 의하여 관련 국가기관에서 통합된 위원회의 정책에 따르기로 하였다. 미국의 정보보호 관련 주요 정책, 법 제도와 그 시행을 연도별로 살펴보면 다음과 같다.

- 1980년 : A Plan for the Evaluation of Trusted Computer Systems
- 1981년 : 컴퓨터보안센터(Computer Security Center, 후에 국가컴퓨터보안센터(National Computer Security Center : NCSC)로 명칭 변경 설립
- 1984년 : NSDD(National Security Decision Directive) 145
- 1985년 : DoD 5200.28-STD "Trusted Computer Systems Evaluation Criteria" [1]

● 1987년 : The Computer Security Act (Public Law 100-235) : 컴퓨터보안법

2.2 영국의 정보보호 관련 정책

영국에서는 1984년 데이타보호법을 제정하여 개인 정보에 대한 보호를 하고 있으며, 상무부는 민수용 IT 제품에 대한 보안 평가를 시행하기 위하여 CCSC를 설립하고 1987년 영국의 민수용 IT 제품에 대한 평가 기준 및 체계에 대한 내용을 기술한 Green Book을 발간하였다. 또한 영국 정부 및 민간 부문에 활용되는 정보보호시스템을 평가·인증하기 위하여 상무부와 CESG가 공동으로 개발한 UK ITSEC (Information Technology Security Evaluation and Certification) Scheme은 유럽의 보안평가 기준서인 ITSEC(Information Technology Security Evaluation Criteria)에 근거하여 평가를 시행하고 있으며 평가승인 결과에 대한 국제적 상호 인증 기반을 제공하고 있다.

2.3 독일의 정보보호 관련 정책

독일에서는 1977년 데이타보호법를 제정하여 개인 데이타에 대한 안전 신뢰성을 확보하기 위한 데이타 보호 조치를 하고 있으며, 1990년 12월 17일 BSI 설립법을 제정 공포함으로써 내무부 소속 기관으로 BSI(Bundesamt für Sicherheit in der Informationstechnik : 독일정보보호원)를 설립하여 정보보호기술의 적용, 정보보호시스템에 대한 평가 기준, 절차 및 도구의 개발, 평가 시행 및 평가필증의 교부 등에 대한 정책적인 시책을 규정하고 있다.

2.4 기타 국외의 정보보호 관련 정책

캐나다는 정보시스템 보안 평가 기준서로 CTCPEC(Canadian Trusted Computer Product Evaluation Criteria) version 1.0을 1989년 첫 발간하여 1993년에 version 3.0을 개정 발간하였고, 이를 체계적으로 수행하기 위한 기관으로 CSE/CCSC를 설립 운영하고 있다. 프랑스와 호주도 ITSEC/ITSEM으로 평가 정책 및 제도를 정립 시행중이며 정보보호 관련 기관으로 프랑스는 SCSSI, 호주는 ANISA를 정부소속기관으로 설립 운영하고 있다.

2.5 국내의 정보보호 관련 정책

1995년 8월 4일 제정 공포된 정보화촉진기본법은 국민 생활의 질 향상과 국민경제의 발전을 도모하기 위하여 국가사회 전반의 정보화 촉진과 정보통신산업진흥 및 정보통신기반 고도화 시책을 범국가적으로 일관성 있고 체계적으로 추진하기 위하여 제정하였으며, 동법 제14조에서 정부는 건전한 정보통신 질서의 확립과 정보의 안전한 소통을 위하여 필요한 정보보호 시책을 효율적으로 추진하기 위한 정보보호센터를 설립 운영할 수 있도록 하였으며, 동법 제15조에서는 정보통신부장관이 정보보호시스템의 성능과 신뢰도에 관한 기준을 고시하고 정보보호시스템의 제조 또는 수입에 대한 기준준수 및 보완을 권고할 수 있도록 규정하고 있다. 또한, 1995년 12월 29일 제정 공포된 정보화촉진기본법 시행령은 정보화촉진기본법에서 위임된 사항과 그 시행에 필요한 사항을 규정하기 위하여 제정된 것으로 센터의 명칭을 한국정보보호센터라 하고 이 센터의 설립, 센터의 운영, 센터의 업무, 시험 평가 등에 관한 사항을 규정하고 있다[2][3].

3. 정보보호 기술

정보화 추진에 따른 부수적 문제점중의 핵심은 바로 정보 자산에 직접적으로 악영향을 미치는 사건으로써 정보 자산과 관련된 정보의 노출사건, 데이타가 중도에서 위, 변조되는 사건, 고의적으로 정보통신 시스템의 장애를 유발하는 사건 및 부정한 방법으로 정보 자산을 사용하는 사건을 들 수 있다. 이러한 보안 문제를 해결하기 위한 연구 개발 및 사용되고 있는 보안기술에는 어떠한 것이 있는지 알아보겠다.

3.1 정보보호관련 위협요소에 대한 기술적 대책

가. 인증(Authentication) 기술

인증이란 자원을 사용하려는 사용자의 신원을 확인하는 것으로써 패스워드와 같은 기본적인 방법에서부터 사용자의 신분을 근간으로 하는 디지탈 서명 방식까지 실로 다양하다 할 수

있으며 키서버를 사용하는 커버로스(Kerberos) 등이 있다[4][5].

나. 접근통제(Access Control) 기술

접근통제란 주체에 대한 객체의 접근을 통제하는 수단으로써 임의적 접근통제(Discretionary Access Control : DAC)와 강제적 접근통제(Mandatory Access Control : MAC)로 나누어진다.

● 임의적 접근통제

임의적 접근통제는 주체나 또는 그들이 소속되어 있는 그룹들의 ID에 근거하여 객체에 대한 접근을 제한하는 방법을 말한다. 즉, 접근통제는 객체의 소유자에 의하여 임의적으로 이루어진다.

임의적 접근통제 메카니즘은 일반적으로 접근통제행렬 모델로 표현되는 것들로 행(row) 중심적 표현형태를 갖는 능력 리스트(Capability List)와 프로파일 그리고 패스워드가 있으며, 열(column) 중심적 표현을 갖는 메카니즘으로는 보호 비트(Protection Bits) 그리고 ACL(Access Control Lists)이 있다.

● 강제적 접근통제

객체에 포함된 정보의 비밀성과 이러한 비밀정보에 대하여 주체가 갖는 정형화된 허가권에 근거하여 객체에 대한 접근을 제한하는 방법을 강제적 접근통제라고 한다. 강제적 접근통제는 주체와 객체가 가지고 있는 보안레이블에 근거하여 객체에 대한 접근 여부를 결정한다[1][6].

- 판독(read) : 주체의 보안등급 ≥ 객체의 보안등급 & 주체의 비밀범주 ≥ 객체의 비밀범주
- 기록(write) : 주체의 보안등급 ≤ 객체의 보안등급 & 주체의 비밀범주 ≤ 객체의 비밀범주

강제적 접근통제를 위한 대표적 보안 모델로는 Bell and LaPadula 모델이 있다[7].

다. 변조방지 기술

정보의 변조방지를 위한 무결성을 제공하기 위하여 전통적으로 CRC 기법에서부터 메시지 다이제스트 기법(예, MD4, MD5), 일방향 해쉬함수(예, Secure Hash Algorithm), 암호기법을 이용한 무결성(예, DES를 이용한 Message Authentication Code)에 이르기까지 그 방법이 다양하다. 정보의 불법적인 수정을 방지하기 위한 단순한 방법으로는 높은 비밀수준의 정보에 대한 기록(Write-Up) 능력을 제거하는 것을 들 수 있다. 그러나 높은 비밀수준 정보에 대한 기록 기능을 제거한다고 해서 정보의 불법적인 수정을 완벽하게 방지하지는 못한다. 컴퓨터 시스템의 대표적인 무결성 모델로는 Biba의 무결성 모델이 있다[7].

라. 인터넷 보안 기술

NII(National Information Infrastructure)의 중추적인 역할을 할 것으로 기대되는 것이 인터넷 프로토콜로 IETF(Internet Engineering Task Force)에서는 차세대 인터넷 프로토콜인 IPv6를 정의하였다[8][9]. IPv6에서 보안 서비스를 제공하기 위하여 "IP Authentication Header(AH)" 및 "IP Encapsulating Security Payload(ESP)"의 두 가지 형태의 특별한 헤더를 이용한다. AH는 IP 데이타그램의 무결성과 암호학적인 기법이 가미되지 않은 인증에 사용된다. ESP는 IP 데이타그램의 무결성, 인증 및 암호화를 제공하기 위해 설계되었다.

또한 전자우편 보안에 사용되는 것으로는 PEM, PGP, TMail, MSP 등이 있고 WWW를 위한 보안 메카니즘으로는 SHTTP, OSF DCE Secure Web 및 Netscape의 SSL 등이 있다. 그리고, Java applets을 위한 보안대책이 마련되고 있다[10].

마. 객체지향 보안기술(CORBA)

CORBA(Common Object Request Broker Architecture)는 개방 환경에서 분산되어 운용되는 응용 프로그램들에 대한 적절한 보호 방법을 지원하기 위해 OMG(Object Management Group)에서 개발하고 있는 객체 응용에 대한 보안 기능이다.

CORBA의 객체 보안 서비스는 다른 객체 서비스들 사이에서 보안 특성인 비밀성, 무결성, 책임성(Accountability), 가용성 등을 만족시킨다. 또한 기능으로는 접근통제 기능, 감사 기능 및 인증 기능을 가진다. 그리고 객체 응용들에 대한 보안 정책도 고려하고 있으며 CORBA의 객체 보안 기능은 사용자뿐 아니라 객체들에 대해서도 적용된다[11].

바. Security API(Application Program Interface)

최근에 이르기까지 암호 기능을 응용 소프트웨어로 통합하는 것은 개발자에게 암호 모듈과 밀접한 관계를 갖도록 하는 것을 요구하였다. 이러한 접근 방식은 응용과 처리해야 할 암호를 각각의 개발 과정에서 새롭게 조합해야만 했으므로 상용 제품을 위해 필요한 모듈성이나 유지보수성을 제공하지 못했다. 따라서, 보다 융통성있고 강력한 대안은 표준화된 CAPI (Cryptographic Application Program Interface)를 사용하는 것이다[10]. 표 1에 각각의 응용 프로그램에 적합한 현재 널리 인정되고 있는 CAPI를 명시하였다.

표 1 응용에 적합한 CAPI

Application	Recommended CAPI
Word Processor	GSS-API
Mail Application	IDUP-GSS-AP
SMTP; X.400	GSS-API
Directory Service; X.500	GSS-API
SNMP; SNMPv2	GSS-API
IPSP; NLSP; TLSP, GULS; MSP	GSS-API
HTTP	GSS-API
Key Management Application	GCS-API
Key Management Protocol	GCS-API
Authentication Application	GCS-API
Security Association Protocol	GCS-API
Certification Manager	GCS-API or Cryptoki
Certificate Manager	Cryptoki
Cryptographic Token Application	Cryptoki

사. 정보보호 기술분류 요약 및 기술현황

앞에서 살펴본 정보보호기술의 제반 분류에 대한 요약 및 현 기술수준을 비교하여 다음의 표 2에 제시하였다.

4. 정보보호 관련 표준화 현황

정보보호에 관련한 표준은 정보기술과 관련한 국제표준화 활동은 분야별로 ISO/IEC JTC1을 중심으로 하는 정보처리 분야의 표준화와 ITU-T를 중심으로 하는 전기통신 표준화로 대별된다. 본 고에서는 ISO/IEC JTC1을 중심으로한 표준화 현황과 국내 현황에 대해서만 기술하기로 한다[12].

JTC1(Joint Technical Committee 1)에는 현재 19개의 분과위원회가 활동 중이며 이중 정보보호 관련 분과위원회로는 SC6(정보통신 및 시스템간 정보교환), SC21(개방형시스템 상호접속, 데이타 관리 및 개방형 분산 처리) 및 정보보호기술을 담당하는 SC27에서 보안 서비스 및 지침, 정보보호 기술 및 메카니즘, 정보보호 평가기준 등에 관한 표준화를 수행하고 있다.

국제 표준화 활동에 대응하여 국내 표준화 활동을 살펴보면, 먼저 ISO 및 ISO/IEC JTC1

표 3 국내 정보보호 관련 표준화 목록

표준번호	제 목	년도	구 분	비고
KS C 5766	64비트 블록 부호 알고리즘의 연산 모드	1986	한국공업규격	
KS C 5767	데이터 부호 알고리즘(DEA) 1 명세	1986	〃	
KS C 5823	정보처리 용어(신뢰도, 유지보수 및 이용도)	1988	〃	
KS C 5817	정보처리 용어(규제, 완전성 및 안전보호)	1990	〃	
KS C 5869	개방형 시스템간 상호접속의 기본 참조 모델—보안구조	1993	〃	
KS C 5884	물리층에서의 데이터 암호화	1993	〃	
KS C 5791	메시지 복원형 디지털 서명 방식	1994	〃	
KS C 5792	블럭 암호 알고리즘을 사용한 데이터 무결성 기법	1994	〃	
KS C 5793	정보보안의 n비트 블럭암호 알고리즘의 운영모드	1994	〃	
KS C 5794	보안기술의 실체인증 기법—제1부 일반모델	1994	〃	
KCS 221	부가형 디지털 서명방식 표준	1996	전기통신표준	
KCS xx	개방시스템 상호접속—수송계층 보안 규약 표준		〃	제정중
KCS xx	800MHz 대역 이동전화 인증 알고리즘 정합 표준		〃	〃

표 2 정보보호 기술분류 및 현황

구 분	세부 구분	국내 현황	세부 구분	국내 현황
1. 정보보호 기초/기반기술 연구	1. 정보보호 이론 연구		2. 정보보호 시스템 분석 이론 연구	
	▶정수론, 선형대수, 타원곡선, 카오스 등	●	▶블럭 암호 시스템	●
	▶복잡도 이론	●	▶스트림 암호 시스템	△
	▶암호의 고속연산	△	▶암호 체계 분석 이론	●
	▶난수의 생성 및 특성 분석 이론	●		
	▶새로운 정보보호 이론 정립 연구	×		
2. 정보보호 핵심기술 연구개발	1. 암호 기술		2. 키 관리 및 키 분배 기술	
	▶암호 시스템 설계	●	▶비밀 키 암호 기법을 이용한 키 관리 방식	△
	▶암호 시스템 평가	△	▶공개 키 암호 기법을 이용한 키 관리 방식	△
	▶고속 암호화 처리	△	▶중앙집중식 키 분배 방식	△
	▶컴퓨터 파일 암호화 유틸리티	×	▶당사자 키 분배 방식	△
	▶DB암호화 유틸리티	×	▶ID기반 키 분배 방식	△
	▶통신망 암호 유틸리티	×	▶키 서버 시스템	×
	▶통신망 데이터 암호 장비	●		
	3. 식별 및 인증 기술		4. 디지털 서명 기술	
	▶일방향 신분확인 방식	△	▶ID기반 디지털 서명	△
	▶양방향 신분확인 방식	△	▶ElGamal형 디지털 서명	△
	▶안전한 해쉬	◎	▶중재 서명 방식	△
	▶영지식 증명 기법 응용	△	▶동시 다중 디지털 서명	△
	▶전산망 인증 프로토콜	△	▶디지털 서명 응용	◎
	▶전산망 인증 서버	×		
	5. 접근통제 기술		6. 침입 탐지 및 추적 기술	
	▶컴퓨터/전산망/DB용 보안 정책	×	▶전산망 침입 탐지 모델	◎
	▶컴퓨터/전산망/DB용 보안 모델	×	▶실시간 침입 탐지 기법	×
	▶컴퓨터/전산망/DB용 접근통제 메카니즘	△	▶실시간 침입 추적 기법	×
	▶컴퓨터/전산망/DB용 접근통제 시스템	×		
	▶단말기 접근통제 시스템	△		
	▶전산망 방화벽 시스템	◎		
	▶전산망 접근통제 서버	×		
	▶보안 유틸리티 S/W	△		
2. 정보보호 핵심기술 연구개발	7. 바이러스/해킹 방지 기술		8. 부인 봉쇄 기술	
	▶바이러스 백신 개발	△	▶비밀 키 암호 기법을 이용한 부인 봉쇄	×
	▶전산망 해킹 기법 연구	◎	▶공개 키 암호 기법을 이용한 부인 봉쇄	×
	▶전산망 해킹 방지 기술	◎		
	▶UNIX보안	△		
	▶인터넷 보안	●		
3. 정보보호 시스템 평가 및 인증기술 연구 개발	1. 평가 모델 연구 개발	◎		
	2. 평가 방법론 연구 개발	◎		
	3. 평가 도구 개발	◎		
	4. 인증 모델 연구 개발	◎		
	5. 인증 방법론 연구 개발	◎		
4. 정보보호 응용 서비스 기술 연구 개발	1. 스마트 카드 응용 기술		2. MHS보안 기술	
	▶전자주민등록 카드	△	▶PEM	△
	▶전자 의료 및 진료	△	▶PGP	△
	▶전자 지갑, 전자 현금의 유통	×	▶Secure MHS	△
	▶전자 결재 서비스	△		
	3. EDI보안 기술		4. 보안 응용 소프트웨어	●
	▶조달EDI보안 서비스	◎		
	▶기업EDI보안 서비스	△		
	▶전자 결재 서비스	△		

●: 체계적으로 진행중, △: 부분적으로 진행중, ◎: 최근 진행 시작, ×: 미비

표 4 ISO/IEC JTC1 정보보호 관련 표준화 목록

표준번호	제 목	년도	위원회	비 고
ISO 8372	Information processing-Modes of operation for a 64-bit block cipher algorithm	1987	SC27	KS C 5767
ISO 9160	Information processing-Data encipherment-Physical layer interoperability requirements	1988	〃	KS C 5884
ISO/IEC 9796	Information technology-Security techniques-Digital signature scheme giving message recovery	1991	〃	KS C 5791
ISO/IEC 9797	Information technology-Security techniques-Data integrity mechanism using a cryptographic check function employing a block cipher algorithm	1994	〃	KS C 5792
ISO/IEC 9798-1	Information technology-Security techniques-Entity authentication mechanisms-Part 1 : General model	1991	〃	KS C 5794
ISO/IEC 9798-2	Part 2 : Mechanisms using symmetric encipherment algorithms	1994	〃	
ISO/IEC 9798-3	Part 3 : Entity authentication using a public key algorithm	1993	〃	
ISO/IEC 9798-4	Part 4 : Mechanisms using a cryptographic check function	1995	〃	
ISO/IEC 9979	Data cryptographic techniques-Procedures for the registration of cryptographic algorithms	1991	〃	
ISO/IEC 10116	Information technology-Modes of operation for an n-bit block cipher	1991	〃	
ISO/IEC 10118-1	Information technology-Security techniques-Hash-functions-Part 1 : General algorithm	1994	〃	KS C 5793
ISO/IEC 10118-2	Part 2 : Hash-functions using an n-bit block cipher algorithm	1994	〃	
ISO/IEC 11770-1	Information technology-Security techniques-Key management-Part 1 : Framework	1996	〃	
ISO/IEC 11770-2	Part 2 : Mechanisms using symmetric techniques	1996	〃	
ISO/IEC 10736	Information processing-Telecommunications and information exchange between systems-Transport layer security protocol	1995	SC6	KSC-초안
ISO/IEC 11577	Information processing-Open Systems Interconnections-Network layer security protocol	1995	〃	
ISO 7498-2	Information processing systems-OSI-Basic Reference Model-Part 2 : Security Architecture	1989	SC21	KC C 5869
ISO/IEC 10164-7	Information technology-OSI-System management : Security alarm reporting function	1992	〃	
ISO/IEC 10164-8	Information technology-OSI-System management : Security audit trail function	1993	〃	
ISO/IEC 10181-1	Information technology-OSI-Security frameworks for open systems : Overview	1996	〃	
ISO/IEC 10181-2	Authentication framework	1996	〃	
ISO/IEC 10181-3	Access control framework	1996	〃	
ISO/IEC 10181-6	Integrity framework	1996	〃	
ISO/IEC 10181-7	Security audit and alarm framework	1996	〃	
ISO/IEC 10745	Information technology-OSI-Upper layers security model	1995	〃	
ISO/IEC 11586-1	Information technology-OSI-Generic upper layers security : Overview, models and notation	1995	〃	
ISO/IEC 11586-2	Generic upper layers security : Security Exchange Service Element(SESE) service definition	1996	〃	
ISO/IEC 11586-3	Generic upper layers security : Security Exchange Service Element(SESE) protocol specification	1996	〃	
ISO/IEC 11586-4	Generic upper layers security : Protecting transfer syntax specification	1996	〃	

조직에 대응한 국내 전문위원회가 국립품질기술원 산하에 조직되어 있고, ITU의 전기통신 표준화와 관련해서는 정보통신부가 ITU에 통신주관청으로 가입되어 있으며, 산하에 한국정보통신기술협회(TTA)가 조직되어 ITU의 표준화 조직에 대응하는 국내 표준화 연구위원회를 운영하고 있다.

이러한 국내의 정보보호 기술 표준화 활동은 이제 시작 단계로써 아직 활성화되어 있지 않은 상황이지만 한국정보보호센터, ETRI, NCA 및 관련학계 등에서 정보보호 관련 표준화 활동을 활발히 추진해 나갈 예정이다. 정보보호와 관련하여 국내 외에서 추진중인 표준화 현황은 표 3, 표 4와 같다.

5. 결 론

본 고에서는 미국, 영국, 독일, 캐나다, 호주, 프랑스 등을 포함하는 최근 국내외 정보보호 관련 정책, 기술 동향 및 표준화에 대한 조사 분석을 기술하였다. 국제적인 정책 및 기술 동향을 살펴본 바와 같이 선진 각국은 정보화 사회의 추진 과정에서 정보보호에 관한 각종의 정책 및 기술을 연구 개발하고 이를 실현하기 위한 효율적인 정보보호체계를 구축해 가고 있다.

국내에서도 개인정보보호를 위한 법 제정, 컴퓨터 범죄에 대비한 형법의 개정, 정보화촉진기본법 제정 등 급속히 변화하고 있는 정보화 시대에 부합하는 정보보호 관련 정책을 실현해 나가고 있다.

이상으로 살펴본 바와 같이 최근의 국내외 초고속정보통신망 확충 등 정보화 진전속도를 고려해 볼 때 국내에서도 다가올 미래의 정보화 시대 발전상을 예측하고, 정보화 촉진을 위한 효율적인 정보보호 관련 정책 및 기술의 연구 개발에 대한 지속적인 노력을 기울여야 할 것으로 사료된다.

참고문헌

1. National Computer Security Center (NCSC), "Department of Defense Trusted Computer System Evaluation Criteria, Department of Defense," DoD 5200.28-STD, Washington, D.C., Dec. 1985.
2. 법률 제4969호, "정보화촉진기본법," 관보 제13080호, '95. 8. 4.
3. 대통령령 제14847호, "정보화촉진기본법시행령," 관보 제13201호, 1995. 12. 29.
4. 정보보호총서, "커버로스와 미시", 한국정보보호센터 제1995-143호, 1995. 10. 9.
5. D. Borman, "Telnet Authentication : Kerberos Version 4", RFC 1411, Jan. 1993.
6. 홍기웅, 이철원, 박태규, 김대호, "안전한 운영체제를 위한 MAC 메카니즘의 설계 및 구현", 정보과학회 추계학술발표논문집, 1990. 10.
7. M. Gasser, Building A Secure Computer System, Van Nostrand Reinhold Company Inc., 1988.
8. R. Atkinson, "IP Authentication Header", RFC 1826, NRL, Aug. 1995.
9. R. Atkinson, ' IP Encapsulating Security Payload", RFC 1827, NRL, Aug. 1995.
10. 홍기웅, "인터넷의 발전과 보안," '96 정보보호심포지움, '96. 7.
11. B. Fairthorne, "OMG White Paper on Security", OMG Security Working Group, Issue : 1.0, Apr. 1994.
12. http : //www.iso.ch/list2, 1997.

이 철 원

1987 충남대학교 수학과(학사)
1989 중앙대학교 대학원 전산학과(석사)
1989～1996 한국전자통신연구소 선임연구원
1996～현재 한국정보보호센터 선임연구원
관심분야 : 컴퓨터·네트워크 보안, 정보보호시스템 기준·평가, 정보보호기술 표준화

홍 기 융

1982 전남대학교 전산학과(학사)
1985～1995 한국전자통신연구소 선임연구원
1990 중앙대학교 대학원 전산학과(석사)
1992～93 이테리, Alenia Spazio사 Senior Researcher
1994 정보처리기술사
1995～1996 한국전산원 선임연구원
1996 이주대학교 컴퓨터공학과(박사)
1996～현재 한국정보보호센터책임연구원, 응용연구팀장, 기준개발팀장
관심분야 : 컴퓨터·네트워크 보안, 정보보호시스템 기준·평가, 정보보호기술 표준화

김 학 범

1988 경기대학교 전자계산학과(학사)
1990 중앙대학교 대학원 전산학과(석사)
1991～1996 한국전산원 주임연구원
1996～현재 아주대학교 대학원 컴퓨터공학과 박사과정재학중, 한국정보보호센터 주임연구원
관심분야 : 컴퓨터·네트워크 보안, 정보보호시스템 기준·평가, 정보보호기술 표준화

이 경 구

1982 한양대학교 무기재료공학과(학사)
1986 Univ. of Central Arkansas Computer Science(학사)
1988 Univ. of Arkansas Computer Science(석사)
1996 Kent State Univ. Computer Science(박사)
1996～현재 한국정보보호센터 선임연구원
관심분야 : 컴퓨터·네트워크 보안, 정보보호시스템 기준·평가, 라우팅 알고리즘, Interconnection Network

오 경 희

1988 서강대학교 전산학과(학사)
1992 한국과학기술원 전산학과(석사)
1992～1996 한국통신 멀티미디어 연구소
1996～현재 한국정보보호센터 주임연구원
관심분야 : 컴퓨터·네트워크 보안, 정보보호시스템 기준·평가, 데이터베이스 보안, 컴퓨터 감사

심 주 걸

1979 중앙대학교 전자공학과(학사)
1991 건국대학교 대학원 전자공학과(석사)
1997～현재 성균관대학교 정보공학과 박사과정 재학중, 한국정보보호센터 기준평가부장
관심분야 : 정보보호시스템 기준·평가, 암호이론