通信情報保護學會誌
第8卷 第1號, 1998. 3

정보보호 기술 분류

김 기 현*, 은 유 진*, 이 인 수*, 이 홍 섭**

요 약

본 고에서는 정보통신망에서 이용되는 정보보호 기술개발에 필요한 기술 분류에 대한 내용을 고찰하였다. 먼저 정보보호기술의 특성을 정의하고, 정보통신망 위협요소와 문제점을 살펴본 후, 이를 방지하기 위한 기술적 대책을 정리하였다. 위의 기술적 대책에 대하여 기술 특성별로 상세기술을 정의하고 이를 분류하였으며, 현재 정보보호 제품의 동향을 파악하였다. 본 기술분류에 대한 활용은 기술개발의 선정이나 중장기 계획수립에 일익이 되기를 기대한다.

1. 서 론

정보통신기술의 발달로 인해 공공·민간분야에서의 정보시스템 사용이 증가하고 있는 반면 인터넷 등 개방형 정보통신망과의 상호접속으로 인하여 정보유출, 파괴, 위·변조, 바이러스 유포 등의 각종 해킹 및 컴퓨터 범죄 증가하고 있다. 반면 정보통신망이 국제적으로 확장됨에 따라 발생하고 있는 새로운 형태의 사이버테러 및 정보전 등에 대한 대비와 전자상거래, 전자화폐 등 새롭게 나타나는 정보통신서비스의 실효성을 확보하기 위해서는 정보보호가 필수적으로 요구된다.

또한 WTO 체제 출범, OECD 가입과 같은 국제적 환경 변화를 수용하면서 이에 능동적으로 대처하며 ISO/IEC community, ITU-T, ITU-R 등 국제 표준화 기구에서 추진하고 있는 정보보호 기술표준화에 국내 기술이 적극 반영될 수 있도록 하기 위해서는 세계 정보보호산업을 주도할 수 있는 최첨단 수준의 정보보호기술 확보가 필요하다.

본 고에서는 정보통신망에서 사용되는 정보보호 기술을 분류하고, 현재의 제품 기술 현황을 고찰한다. 먼저 정보보호기술의 특성을 고찰하고 정보화 추진에 의하여 부수적으로 발생가능한 문제점 및 그 문제점을 유발하는 안전 위협요소와 기술적 대책을 기술한다.

2. 정보보호 기술의 특성

현재 정보보호 기술은 정보산업계의 필수 불가결한 핵심 요소 기술로써, 비록 공개되고

* 한국정보보호센터 기술본부 연구원
** 한국정보보호센터 기술본부장

공유되고 있으나 핵심기술은 국가 안보적 차원에서 접근되고 있으며 국가별 여건에 따라 중요 핵심 기술은 여러 형태로 수출입을 규제하고 있다. 이처럼 정보보호 기술은 다른 기술과 달리 다음과 같은 특성을 지니며 국내 독자적인 핵심기술을 개발·확보가 요구되는 기술이다.

○ 특수성(국가환경 종속성)
핵심 기술의 수출입 규제 등 국가안보상 각국의 실정에 크게 의존하는 분야임

○ 독자성
국내의 전산망 환경을 해외 기술제품만으로 적절하게 대처하기에는 많은 어려움과 부작용이 따르므로 독자적 기술개발이 요구되는 분야임

○ 고부가가치성
미래의 정보통신 산업의 안전성 보장을 위한 핵심산업으로 희소가치성에 따라 고부가가치가 예상되는 분야임

○ 사회성
독자적으로 침해사고 대응환경을 구축하고, 필요에 따른 상호협력 관계 유지가 요구되는 분야임

○ 기반특성
국가 중요정보기반구조 보호를 위하여 필수적으로 요구되는 분야임

3. 위협요소 및 대책

일반적으로 위협은 다음과 같이 분류된다[2].

○ 실수 및 태만(Error and Omission)
○ 사기 및 절도(Fraud and Theft)
○ 피고용인의 사보타지(Employee sabotage)
○ 물리적 및 기반 손실(Loss of Physical & Infrastructure Support)
○ 악의적인 해커(Malicious Hackers)
○ 산업스파이(Industrial Espionage)
○ 악의적인 코드(Malicious Code)
○ 외국정부스파이(Foreign Government Espionage)
○ 개인 프라이버시 침해(Threats to Personal Privacy)

이러한 위협은 정보통신망에서 도청, 신분위장, 전송 메시지의 내용 부인, 부당 목적 소프트웨어 은닉, 시스템 보안 관리 미비 등의 안전 위협요소로 나타나며 정보자산에 직접적으로 악영향을 미치는 사건 즉, 정보자산과 관련된 정보의 누출(Information leakage), 데이터의 위·변조(Integrity violation), 시스템 장애 유발(Denial of service) 및 정보자산의 부정사용(Illegitimate use) 등의 형태로 나타난다[1].

○ 도청
송수신 양단간의 통신선로 또는 통신기기의 전자파를 수집하여 정보를 유출하는 방식

○ 신분위장
자신의 신분을 정당한 사용자(타인)의 명의로 위장하여 시스템에 침투, 비인가된 정보를 열람, 위변조하거나 송·수신중 통신선로를 조작한 후 정당한 송·수신자에 허위정보를 전송하여 통신내용을 가로채는 행위

○ 전송메시지 내용
정당한 방법으로 메시지를 송신 또는 수신한 후, 고의적으로 메시지의 내용을 부정하는 행위

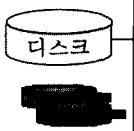
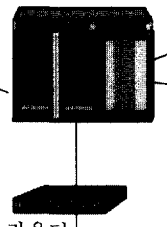
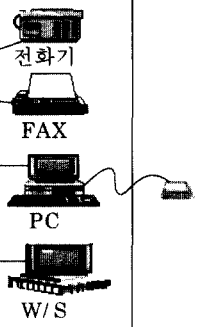
○ 부당 목적 S/W 은닉

정보통신망의 안전성을 저해할 목적으로 통신서버 등의 중요한 컴퓨터에 트로이 목마, 트랩도어, 악성 바이러스 등을 은닉하는 행위

○ 시스템 보안 관리 미비

시스템의 보안관리 대책이 미비하거나 관리자 또는 사용자가 관리대책을 준수하지 않아서 정보통신망 또는 컴퓨터 시스템의 안전을 저해하는 사건

위에서 언급한 안전 위협요소에 대하여 일반적으로 관리적 측면과 기술적 측면으로 대책을 수립하여 문제점을 해결한다. 여기서 기술적 측면에서 사용되는 기술로는 크게 인증기술(Authentication), 접근통제기술(Access Control), 정보내용 보호기술(기밀성,

	데이터 저장장치	호스트 컴퓨터 응용 프로그램	유선망 무선망 위성통신망	교환기 라우터	전화기 FAX PC W/S	카드
정보보호대상						
위협요소	데이터/파일 삭제, 복사, 수정	OS 취약점 응용프로토콜 취약점 서비스 거부 바이러스 재시도 공격 EMI/EMC	도청 데이터위변조 EMI/EMC	프로토콜 취약점 프래픽 폭주	신분위장 EMI/EMC	신분위장 카드복제
기술적 대책	접근제어기술 Secure DBMS	사용자 인증기술 취약성 진단기술 GSS-API 전자서명 TEMPEST 바이러스 방지 기술 Secure OS	비밀키 암호 공개키 암호 해쉬함수	취약성 진단기술 Secure 라우터	사용자 인증기술 TEMPEST	사용자 인증기술 Secure COS 고속 암호칩

(그림 1) 위협요소 및 기술적 대책

Confidentiality), 데이터 위변조 방지 기술(Integrity), 데이터 내용 부인봉쇄 기술(Non-repudiation) 등을 들 수 있다[1].

○ 인증기술
송·수신자가 상대방의 신원을 확인, 식별하는 기술

○ 접근통제 기술
비인가자가 정보통신망 자산을 부정한 방법으로 사용하는 것을 방지하는 기술

○ 정보내용 보호기술
비인가자가 부당한 방법으로 정보를 입수한 경우에도 정보의 내용을 알 수 없도록 하는 기술(암호기술 등)

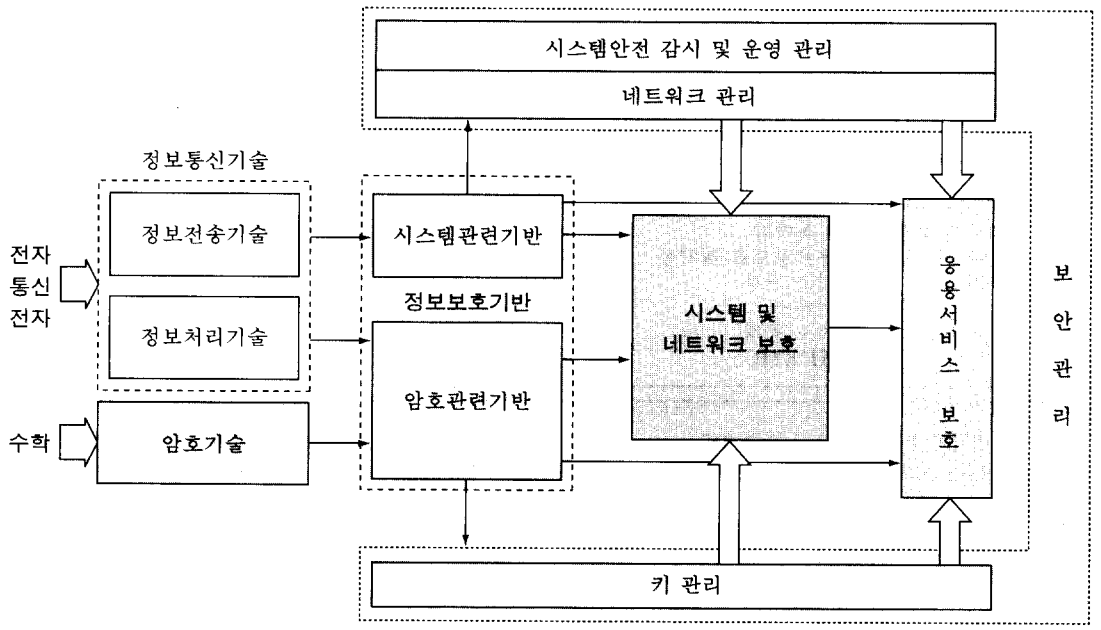
○ 데이터 위·변조 방지기술
데이터가 전송 도중 또는 데이터베이스에 저장되어 있는 동안 악의의 목적으로 위조 또는 변조되는 것을 방지하는 기술

○ 데이터 내용 부인봉쇄 기술
송수신 당사자가 각각 전송된 데이터의 내용을 추후 부인하는 것을 방지하는 기술

본고에서는 이러한 위협요소를 호스트 컴퓨터, 데이터베이스, 네트워크 등 정보통신망에서의 정보자산에 대한 위협의 형태로 분류하고 이에 대한 세부적 기술적 대책을 (그림 1)과 같이 나타내었다.

4. 정보보호기술 분류

정보보호 기술은 기반기술, 핵심기술, 응용기술로 분류하기도 하며 크게 기반기술과 응용기술로 분류하기도 한다[3,4]. 또한 정보보호 서비스를 제공하기 위한 측면에서 인증기술,



(그림 2) 분야별 정보보호 기술분류

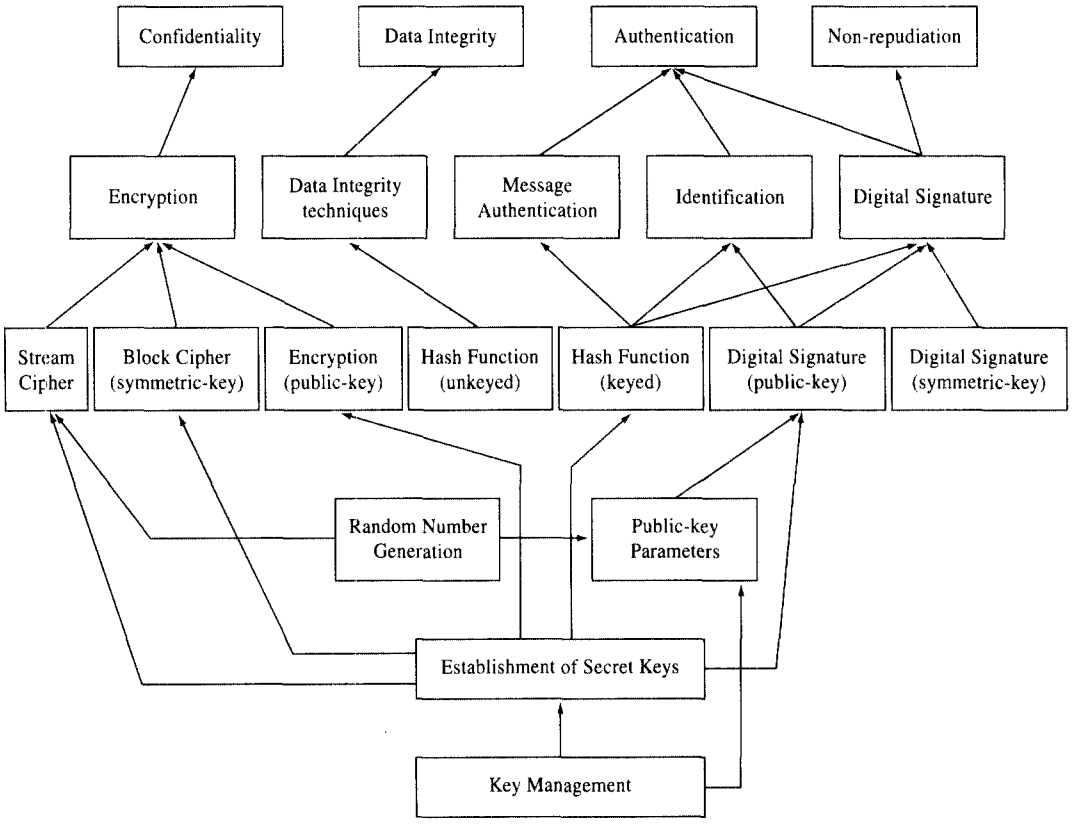
접근통제 기술, 데이터 내용 보호기술(암호화 기술), 위·변조 방지기술(무결성), 데이터 내용 부인봉쇄 기술로 분류하기도 한다[1].

본 고에서는 정보보호관련 자료들에서 나타난 기술 특성을 고려하고 대분류의 정보보호 기술을 보다 세분화하여 (그림 2)와 같이 정보보호 기반 기술, 시스템 및 네트워크 보호 기술, 응용서비스 보호 기술 그리고 보안관리 기술로 분류하고 이를 기술한다.

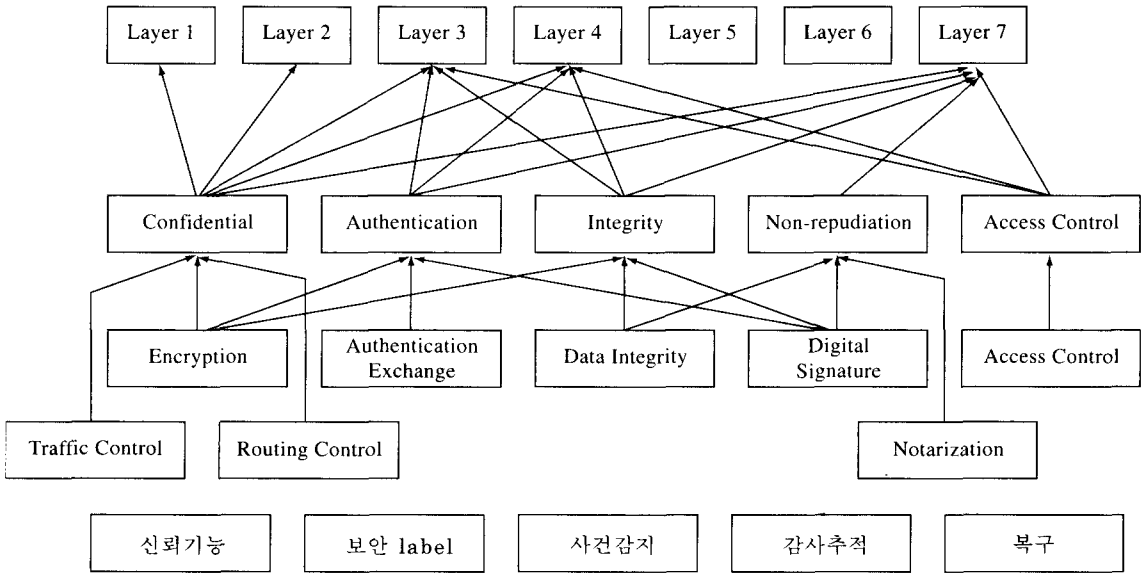
가. 정보보호 기반기술

정보보호 기반기술의 분류에 앞서 정보보호 기술에서 기반기술로써 중요한 위치를 차지하고 있는 암호기술과 컴퓨터 보호 및 네트워크 보호기술에서의 기반기술로써 논하고 있는 기술을 먼저 고찰하고자 한다.

먼저 암호기술은 기밀성, 무결성, 인증 및 부인봉쇄 서비스를 제공하기 위한 기술들로 (그림 3)[5]과 같이 분류된다. 암호기술에서는 주요 암호 알고리즘, 암호 프로토콜을 나타내고 있으며 보안 관리부분으로 키관리 기술이 중요한 위치를 차지하고 있다. 그 외 구현이나 응용은 부분적으로 다루고 있다. 본 고에서는 암호기술 중 암호 알고리즘 및 암호 프로토콜 관련 기술을 정보보호 기반 기술로써 다루며 키관리 기술은 보안관리 부분에서 기술한다.



(그림 3) 암호기술 분류



(그림 4) 네트워크 보호를 위한 기본 기술

그 외 구현이나 응용부분은 시스템 및 네트워크 보호 또는 응용서비스 분야에서 다룬다.

컴퓨터 보호기술에서는 식별 및 인증, 부정접속 방지, 접근통제, 감사증적, 정보흐름통제 기술 등이 기반을 이루고 있다[6,7].

- ○ 식별 및 인증 기술 : 기억, 소유, 특성 등을 이용
- ○ 부정접속 방지기술 : 대화(Dialog) 방식, Call-back 방식, 암호기반방식 등
- ○ 접근통제 기술 : 임의적 접근통제 기술, 강제적 접근통제 기술
- ○ 감사증적 기술 : 확인기록, 보안위배사항 검출, 감사추적 등
- ○ 정보흐름통제기술 : Lattice 보안모델, 불법 정보흐름채널(Covert Channel) 방지 기술 등

컴퓨터 보호기술에서의 정보보호 기반기술은 무결성 및 기밀성을 제공하기 위한 암호기술을 제외하고는 대부분 정보처리기술 즉, 시스템 기술에 그 기반을 두고 있다.

마지막으로 네트워크 보호기술은 ISO/IEC 7498-2[8]에서 네트워크에 정보보호 서비스를 제공하기 위하여 암호화, 인증교환, 데이터 무결성, 디지털 서명, 접근제어, 부인봉쇄, 트래픽 제어, 라우팅 제어, 신뢰기능, 보안 레이블, 사건 감지, 감사 추적, 복구 기술 등이 기반을 이루어 있으며 요약하면 (그림 4)와 같다. 여기에서 암호화, 인증교환, 데이터 무결성, 디지털 서명 기술은 암호기술에 기반을 두며 접근제어, 부인봉쇄, 트래픽 제어, 라우팅제어 기술 등은 정보처리기술 및 정보전송기술에 기반을 둔다.

위에서 고찰한 바와 같이, 정보보호 기반기술은 이론적 암호학이나 정수론 등 암호기술에 정보처리 기술이 가미되어 암호 알고리즘, 암호 프로토콜 기술을 형성하고 있는 암호 관련 기술과 감사기록, 접근제어 등 정보처리 기

술 및 라우팅 제어, 트래픽 제어 등 정보전송 기술에 기반을 둔 순수 시스템 관련 기술로 구분된다.

○ 암호관련 기술
순수 암호기술 및 정보처리 기술에 기반을 둔 정보보호 기반기술

- 순수 암호학 및 계산적 정수론
- 암호 알고리즘 및 분석 : 비밀키 암호, 공개키 암호, 해쉬함수, 암호분석, 난수생성 등
- 암호 프로토콜 : 인증 프로토콜, 키교환 프로토콜, 디지털 서명 프로토콜, 영지식 프로토콜 등

※ 암호 알고리즘 : 하나 이상의 비밀 매개변수를 사용하여 데이터의 정보 내용을 해독할 수 없도록 변환하거나 그렇게 변환된 내용을 다시 원문으로 환원시키기 위해 데이터를 변형시키는 것
※ 암호 프로토콜 : 특별한 정보보호 목적을 얻기 위하여 두 개 또는 그 이상의 실체에 요구되는 행위를 정확하게 규정하는 일련의 스텝으로 정의되는 분산된 알고리즘

○ 시스템관련 기반
정보처리 기술 및 정보전송 기술에 기반을 둔 정보보호 기반기술

- 정보처리기반 기술 : 식별 및 인증 기술, 부정접속 방지기술, 접근통제 기술, 감사 증적 기술, 정보흐름통제기술 등
- 정보전송기반 기술 : 경로제어 메카니즘, 트래픽 패딩 메카니즘 등

※ 정보보호 메카니즘 : 정보보호 기능을 소프트웨어나 하드웨어 상에 구현하기 위한 논리 및 알고리즘

나. 시스템 및 네트워크 보호

일반적으로 시스템 및 네트워크 보호기술은 통신 보호, 네트워크 보호, 컴퓨터 보호 기술로 구분되며 다음과 같이 정의된다.

○ 통신 보호(COMSEC)
- 정보가 전송되는 동안 인가되지 않는 노출, 변경, 파괴로부터 보호하는 것
- 암호시스템을 이용하여 불안전한 자료 채널상에서 통신망 내의 두 지점 사이에 안전하게 정보를 송수신하는 기술

○ 네트워크 보호(NETSEC)
- 인가되지 않은 노출, 변경, 파괴로부터 네트워크, 네트워크 서비스 및 네트워크 상의 정보를 보호하는 것
- 네트워크의 중요한 기능이 정확히 수행되는지, 해로운 효과가 존재하는지, 정보가 정확한지를 보증하기 위한 기술

○ 컴퓨터 보호(COMPUSEC)
- 인가되지 않은 노출, 변경, 파괴로부터 정보시스템에서 처리 보관되는 정보를 보호하는 방법

반면, 미국방부 내 보안센터인 NCSC (National Computer Security Center)에서는 시스템 및 네트워크 관련 제품을 COMSEC, TEMPEST, COMPUSEC의 3가지 분야로 구분하여 평가·승인하며 이를 살펴보면 다음과 같다[11].

○ COMSEC

전화, 마이크로웨이브, 위성 등의 전송로 상에서 비인가된 정보의 접근, 노출, 수집, 조작, 수정을 방지하기 위한 기술

○ TEMPEST

정보기기 각 부품의 전자파 방출을 감지하여 정보를 뽑아내는 것을 방지하기 위하여 제한된 정도의 허용치를 지닌 부품을 개발하는 기술

○ COMPUSEC

컴퓨터나 네트워크내에 축적 또는 처리하는 정보의 비인가된 접근, 노출을 방지하기 위한 기술

오늘날 통신보호는 전송매체의 특성에 따른 위협요소에 대한 보호대책만을 의미하는 경우가 많으나 정보통신매체라는 관점에는 전송매체뿐만 아니라 시스템 자체의 EMI/EMC (Electro- Magnetic Interference/Electro-Magnetic Compatibility) 또한 큰 위협요소로 분류한다. TEMPEST는 때로 COMSEC에 포함되기도 하나 COMSEC에서는 시스템 자체의 전자파 방출에 대해서는 다루지 않는다. 또한 개방통신망 환경에서 컴퓨터 보호는 단일 호스트에서의 정보보호뿐만 아니라 다중 호스트에서의 정보보호까지 포함하면서 네트워크 보호까지 다루고 있다. 과거 통신보호은 전화, 위성 등 전송로에서의 음성통신보호가 주를 이루었으며 네트워크 보호는 컴퓨터 시스템을 연결하는 네트워크에서의 데이터 보호를 다루었다. 하지만 정보통신이 발달하면서 통신과 네트워크의 관계가 애매해지고 있다.

본 고에서는 OS 보호, DBMS 보호 등 단일 호스트에서의 정보보호를 컴퓨터 보호기술로, 다중 호스트 및 네트워크에서의 정보보호를 네트워크 보호기술로, 전송매체의 위협요소 및 시스템의 전자파 방출을 방지하기 위한 기술을 통신보호 및 TEMPEST로 그 특성을 제한하여 분류한다.

○ 통신보호 및 TEMPEST

- 전송로 상에서 비인가된 정보의 접근, 노출, 수집, 조작, 수정을 방지하기 위한 기술 및 정보기기 각 부품의 전자파 방출을 감지하여 정보를 뽑아내는 것을 방지하기 위한 기술
- 회선보안, 전송보안, EMI/EMC, Emanation Security 등

○ 네트워크 보호

- 다중 호스트 및 네트워크에서의 정보보호로 인가되지 않은 노출, 변경, 파괴로부터 네트워크, 네트워크 서비스 및 네트워크 상의 정보를 보호하는 것
- 각 계층별 통신 프로토콜, LAN 보호, 인터넷 보호, 초고속망 보호 기술 등

○ 컴퓨터 보호

- 단일 호스트에서 정보보호로 인가되지 않은 노출, 변경, 파괴로부터 정보시스템에서 처리 보관되는 정보를 보호하는 방법
- 파일 시스템 보호, 데이터베이스 보호, OS 보호, PC 보호, 바이러스 방지 기술 등

다. 응용서비스 보호

응용서비스 보호기술은 정보보호 기반 및 시스템/네트워크 보호기술들을 활용하여 정보통신 응용서비스에 정보보호 기능을 제공하는 기술을 의미한다. 본 고에서는 현재 제공되고 있는 응용서비스 뿐만 아니라 초고속정보통신

기반에서 예상되는 응용서비스까지 포함하여 분류한다. 미국의 경우 NII(National Information Infrastructure)에서 가능한 응용서비스를 다음 6가지 측면으로 분류하고 위험성을 분석하였다[13].

○ 게임/비디오/CD-ROM/SW 등을 포함한 오락서비스
○ 건강/교육 관련 서비스
○ 재정/보험/상업 서비스
○ 지능형 교통/운송 서비스
○ 정부 정보서비스
○ 공중망
○ 인터넷

국내에서는 KII(Korea Information Infrastructure)에 적합한 응용서비스로 다음과 같이 5가지를 고려하고 있다[12].

○ 전자상거래
○ 가상학교
○ 분산 경영서비스
○ Telegovernment
○ Smart Application

(참고 12)에서는 NII의 6가지 서비스와 KII의 5가지 서비스를 비교하여 Telegovernment를 정부 정보서비스 차원으로, 분산경영을 전자상거래 차원으로, Smart Application을 원격 오락/의료/교육서비스 차원으로 그 범위를 확장시켜 7가지 서비스로 구분하였다. 본고에서는 (참고 12)에서 분류한 7가지 서비스를 응용서비스로 분류한다.

○ 전자상거래 보호
- 홈쇼핑, 전자무역거래, CALS, EDI 등

○ 정부서비스 보호
- 우체국, 동사무소, 세무서, 구청 등

○ 의료 및 보건 서비스 보호
- 의료, 보건, 건강 등

○ 금융 및 재정서비스 보호
- 금융, 재정, 보험 등

○ 교통 및 운송서비스 보호
- 여행, 교통, 일기 등

○ 교육서비스 보호
- 학습, 교육, 세미나, 훈련 등

○ 오락서비스 보호
- 음악, 영화, 게임, 소프트웨어 등

라. 보안관리

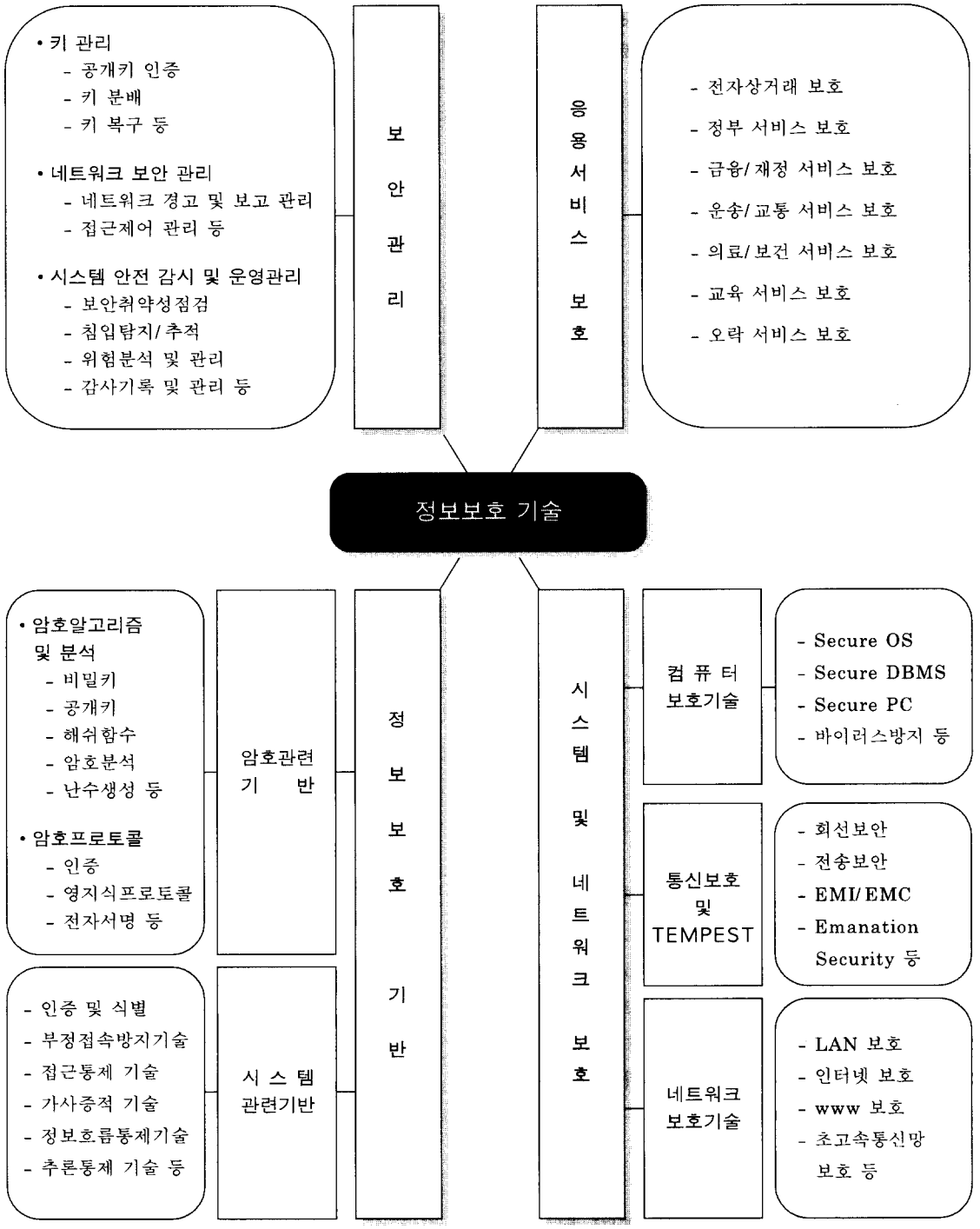
보안관리는 정보보호 기능의 안전하고 효율적인 지원, 유지, 및 운영을 위하여 필요한 관리 기술로써 키 관리, 네트워크 보안 관리, 시스템 안전 감시 및 운영관리 등이 있다.

○ 키관리
- 공개키 인증, 키분배, 키복구 등

○ 네트워크 보안관리
- 네트워크 보고 및 경고 관리, 접근제어 관리 등

○ 시스템 안전 감시 및 운영관리
- 시스템 보고 및 경고 관리, 보안취약점 점검, 침입탐지 및 추적, 위험 분석 및 관리, 감사기록 및 관리 기술 등

6. 정보보호 기술 분류 요약



(그림 5) 정보보호기술 분류 요약도

7. 정보보호 기술 및 활용 분야

구 분			기 술	활용분야
정보보호 기반	암호관련 기반	암호알고리즘 및 분석	비밀키 암호	시스템 및 네트워크 보호기술, 응용서비스 보호기술 등에 활용
			공개키 암호	
			해쉬함수	
			암호분석	
			난수생성 등	
		암호프로토콜	인증 프로토콜	인증 제품 스마트 카드 암호 제품 등
			키교환 프로토콜	
			디지털 서명 프로토콜	
			영지식 프로토콜 등	
	시스템 관련 기반		식별 및 인증 기술	시스템 및 네트워크 보호기술, 응용서비스 보호기술 등에 활용
			부정접속 방지 기술	
			접근통제 기술	
			감사증적 기술	
			정보흐름통제 기술	
			추론통제 기술	
			트래픽 제어 기술	
			라우팅 제어 기술 등	
네트워크 및 시스템 보호	통신보호 및 TEMPEST		회선 보안	음성통신 보호, 이동통신 보호, 위성통신 보호, TEMPEST 등
			전송 보안	
			EMI/EMC	
			Emanation Security 등	
	네트워크 보호기술		통신프로토콜	SILS, SP3/4, NLSP, IPv6, SSL, SHTTP, Kerberos, SESAME 등
			LAN 보호 기술	
			인터넷 보호	
			초고속망 보호 등	
	시스템 보호 기술		Secure OS	Secure OS Secure DBMS PC 보호 바이러스 백신 등
			Secure DBMS	
			PC 보호	
			바이러스 방지 기술 등	

응용서비스 보호		전자상거래 보호	정부서비스 의료/보건 서비스 금융/재정 서비스 교통/운송 서비스 교육 서비스 오락 서비스 등
		정부서비스 보호	
		의료/보건 서비스 보호	
		금융/재정 서비스 보호	
		교통/운송 서비스 보호	
		교육 서비스 보호	
		오락 서비스 보호 등	
보안관리	키 관리	공개키 인증	키관리 시스템 및 기반구조 구축에 활용
		키 분배	
		키 복구 등	
	네트워크 보안관리	네트워크 경고 및 보고 관리	네트워크 보안 관리 시스템 등
		접근제어 관리 등	
	시스템 안전감시 및 운영관리	보안 취약성 점검	취약성 점검 도구 침입탐지/추적 시스템 위험분석 및 관리 시스템 감사기록 및 관리 시스템 등
		침입탐지 및 추적	
		위험 분석 및 관리	
		감사기록 및 관리 등	

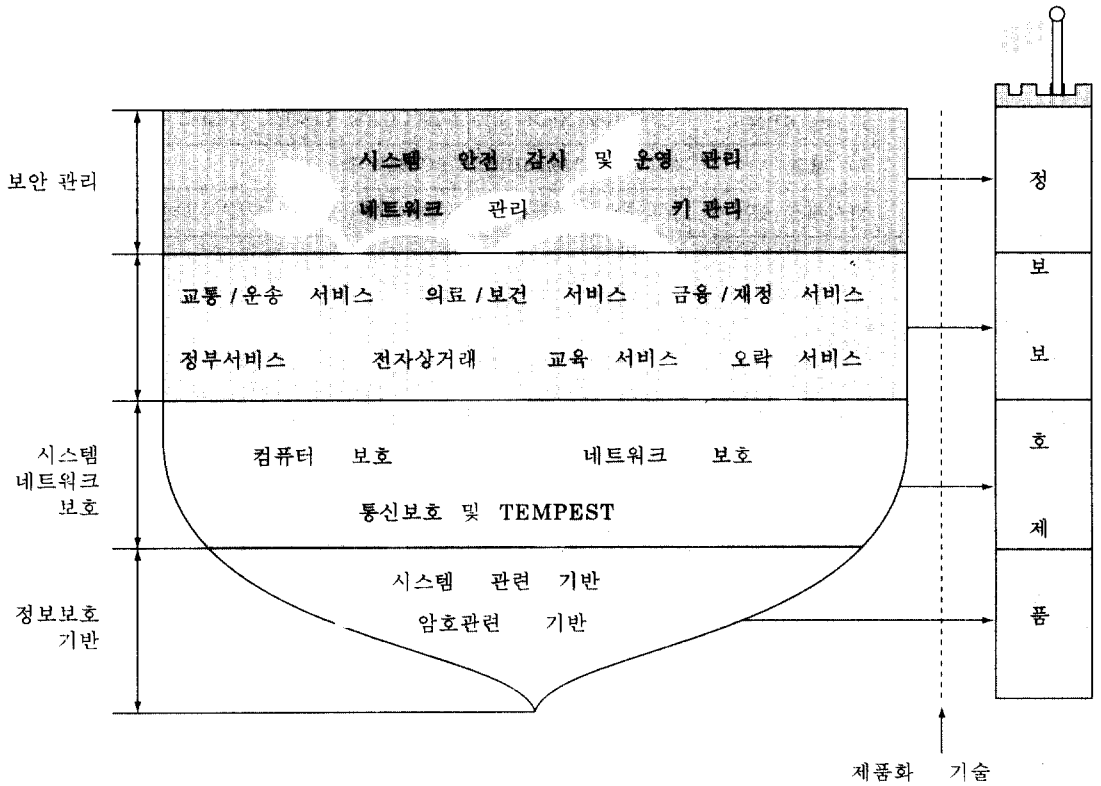
8. 정보보호 제품기술

일반적으로 정보보호 제품은 침입차단시스템, 바이러스 방지, 사용자 식별 및 인증, 접근통제, 암호화, 시스템 안전감시 및 운용관리 제품, 물리적 보안 제품으로 분류한다[10]. 하지만 이들 정보보호 제품은 상용 보안제품들이며 이외에도 보안 OS 제품, 보안 DBMS 제품, 금융 및 전자상거래 보호 제품, 네트워크 보호 제품 등이 있다[11]. 본 고에서는 상용정보보호 제품 뿐만 아니라 다른 정보보호제품까지 포함하여 제품기술을 나타내기 위하여 정보보호 제품기술을 (그림 6)과 같이 정보보호기술이 제품화 기술을 통하여 정보보호 제품의 형태로 나타나는 것으로 정의한다.

가. 정보보호기반 기술

정보보호기반 기술 관련 제품들은 암호관련 기술에 기반을 제품들이 대부분이며 시스템

구 분		제 품
암호관련 기반	비밀키 암호	DEF, EastLock, Microcrypt, DES Module, DES32 등
	공개키 암호	RSA Chip, Crypt Master, BSAFE, RSA 512, SIFR 등
	인증	OnceID, S/Key, SecureID, OPIE, PathKey 등
시스템관련 기반	접근통제방지	TCP Wrapper, Call-Back Modem 등



(그림 6) 정보보호기술 총괄 개념도

관련 기반 기술은 시스템 및 네트워크 보호 제품, 응용서비스 제품, 보안관리 제품 형태로 나타난다. 정보보호기반 기술 관련 제품으로는 암호화 제품, 인증 제품 등의 암호관련 기반 제품과 시스템 및 네트워크 보호특성을 지닌 접근통제제품등 시스템관련 기반 제품이 있다.

나. 시스템 및 네트워크 보호

시스템 제품으로는 보안 OS, 보안 DBMS, 바이러스 백신 등이 있으며 네트워크 보호 제품으로는 침입차단시스템, 보안 LAN 등이 있다.

구 분		제 품
통신보호 및 TEMPEST	음성통신	PriveFone, CDS, DST-400, Security Telephone Devices 360 등
	FAX 통신	PrivaFax, Secure FX, Security Facsimile Devices 3700 등
	MODEM	Secure ZMODEM, DES MODEM, MODEM Lock 등
	이동통신	Security Cellular Telephone 9300 등
네트워크 보호	침입차단시스템	수호신, InterGuard, 매직캐슬, 화랑, Secure Shied Firewall, Gauntlet-K, Firewall-1 등
	LAN 보호	MLS LAN Secure Network Server, VSLAN 등

컴퓨터 보호	Secure OS	AIX CMW, MVS/ESX, OS400, SYSTEM V.MLS 등
	Secure DBMS	INFORMIX-ON LINE/SECURE, Oracle7, Trusted cracle7 등
	PC 보호	PCVault, MemoHASP, PC-Safe 등
	바이러스 방지	V3, KAV, 키콥, 타키온, PC 시린, VFind, AVP, ViruSafe 등

다. 응용서비스 제품

응용서비스 제품으로는 주로 전자상거래 관련 전자화폐, 홈뱅킹, EDI, CALS 등이 있다.

구 분		제 품
응용서비스 보호	신용카드 응용	FV, CyberCash, SmartWallet, iKP, CFWallet 등
	네트워크 신용보증	Netcheque, NetBill 등
	전자현금	Ecash, NetCash, CAFE 등

라. 보안관리 제품

보안관리 제품으로는 키관리를 위한 제품

구 분		제 품
키관리		SC 3000, EFTLINK, CIS 등
네트워크 관리	침입차단시스템	수호신, InterGuard, 매직캐슬, 화랑, Secure Shied Firewall, Gauntlet-K, Firewall-1 등
	LAN 보호	MLS LAN Secure Network Server, VSLAN 등
시스템 안전감시 및 운영관리	시스템 취약성 점검	SecuDr, COPS, SATAN, ISS, Doc, checkXuers, Tiger 등
	침입탐지 및 추적	IDES, Haystack, ASAX, GrIDS, NID, CMDS, NADIR 등
	위험분석 및 관리	RiskPAC, NetRisk, BankCheck 등
	감사기록 및 운영기록 확인	Argus, Arpwatch, Checklastlog, RIACS, Swatch 등

마. 기타

위에서 언급한 제품 기술이외에 주요 시설물로의 접근통제를 위한 제품, PC 등 하드웨어를 보호하기 위한 장치 등 물리적 보안 제품이 있으며 인증 서비스 및 평가 서비스를 제공하기 위한 서비스 관련 기술 등이 있다.

기술, 시스템의 작동감시 및 침입탐지 등 시스템 안전운영 및 감시 제품들이 있다.

6. 결 론

최근의 정보통신 분야에서 정보보호는 과거의 선택 사항에서 필수 사항으로 옮겨 가고 있다. 즉, 보호해야 할 정보의 가치와 대상이 증가하고 있다는 의미로써, 예를 들어 전자상거래에서 거래내용과 상대방의 인증 및 확인 등, 정보보호 기술을 이용하지 않고는 결코 활성화가 될 수 없다는 것을 느낄 수 있을 것이다.

정보보호기술은 그 특수성으로 인하여 국내 독자적인 핵심기술의 개발·확보가 필요하며 외국 기술에 의존할 수 없는 민감한 기술로 국내 전산망 환경에 적합한 정보보호 기술개발이 필요하다. 또한 보안사고 예방차원에서의 효율적이고 안정적인 정보시스템의 운영·관리와 침해사고에의 피해로부터 즉각적으로 대응하고 정보자원의 유출 및 파괴, 바이러스, 각종 해킹 및 컴퓨터 범죄로부터 개인/기업 정보의 경제적 피해를 최소화하기 위하여 절실히 요구되는 분야이다.

정보보호기술은 법·제도, 기술표준화, 산업육성, 평가 및 인증, 사고 대응 등 각 영역에서 요구되는 정보보호 목표를 달성하기 위해 필수적으로 요구되는 기술부터 순차적으로 개발하여 이러한 영역들의 수행을 지원해야 할 것이다.

이직도 국내·외에서 정보보호기술에 대한 분류는 70년대 암호기술의 민간부분 활성화부터 시작하여, 활용분야에 따라 통신, 컴퓨터, 수학 등 영역에 따라 차이가 크지만, 본 고에서는 정보통신망에서의 보호대상과 위협요소에 따른 기술적 대책을 중심으로 정리하였다.

향후에는 발전하는 정보통신 및 정보보호 서비스와 안전한 시스템 관리 및 운영 등으로 범위를 확대하여 발전시켜 나가야 할 것이다.

참 고 문 헌

[1] 고승철, 성맹희, "정보보호기술 분류", 정보처리학회지 제4권 제2호, 1997, pp83~90.

[2] An Introduction to Computer Security: The NIST Handbook, NIST.

[3] 정보보호산업발전대책(1998-2002), 정보통신부, 1997.

[4] 정보보호 표준방식 개발, 한국전자통신연구소, 1996.

[5] A. J. Menezes etc., Handbook of Applied Cryptography, CRC Press, 1997.

[6] C.P. Pfleeger, Security in Computing, Prentice Hall, 1989.

[7] S. Castano etc., Database Security, Addison-Wesley, 1994.

[8] ISO/IEC 7498-2, Information Processing Systems - OSI Basic Reference Model - Part 2 Security Architecture, 1989.

[9] Warwick Ford, Computer Communication Security, Prentice Hall, 1994.

[10] 정보보호산업 분류 및 실태 조사, 한국정보보호센터, 1997.

[11] 김석우, "평가승인 보안제품과 최신기술 동향", Security World, 1997. 11., pp113~117.

[12] 초고속정보통신기반 안전성 기술개발, 한국전자통신연구소, 1996.

[13] http://www.ncs.gov, NII Risk Assessment : A Nation's Information at Risk, IITF TPC, 1996.

□ 著者紹介

김 기 현

1993년 경북대학교(공학사, 전자공학과)
1995년 경북대학교(공학석사, 전자공학과)
1995년 7월 ~ 1996년 7월 데이콤 시외전화구축팀
1996년 7월 ~ 현재 한국정보보호센터 기술본부 주임연구원
1997년 10월 ~ 현재 TTA 정보보호기술연구위원회 간사

※ 주관심분야 : 시스템 및 네트워크 정보보호

은 유 진

1995년 아주대학(학사, 컴퓨터공학)
1997년 아주대학교(석사, 컴퓨터공학)
1996년 12월 ~ 현재 한국정보보호센터 기술본부 주임연구원
1997년 10월 ~ 현재 한국정보통신기술협회 정보보호기술 연구위원

※ 주관심분야 : 컴퓨터/네트워크 정보보호

이 인 수

1993년 연세대학교(이학사, 수학과)
1997년 연세대학교(이학석사, 수학과)
1996년 12월 ~ 현재 한국정보보호센터 기술본부 연구원
1998년 3월 ~ 현재 한국정보통신기술협회 정보보호기술 연구위원

※ 주관심분야 : 암호알고리즘 및 키관리

이 홍 섭

1979년 한양대학교(학사, 전자공학)
1985년 한양대학교(석사, 전자공학)
1980년 ~ 1996년 한국전자통신연구소, 연구원 ~ 책임연구원, 실장
1996년 ~ 현재 한국정보보호센터, 연구개발부장, 기술본부장
정보통신기술협회 정보보호분과위원회 의장
한국통신정보보호학회 상임이사

※ 주관심분야 : 시스템 및 네트워크 정보보호