通信情報保護學會誌
第1卷, 第2號, 1991. 8



# 전산망의 안전대책 개요 (I)[1]

이필중[2] · 정진욱[3] · 박명순[4] · 이재용[5]

## 1. 서 론

### 1.1 전산망의 발달 및 구성

이십세기 후반에 들어와서 컴퓨터와 통신의 눈부신 발달로 우리가 살고 있는 세상은 산업화시대에서 정보화 시대로 변환되었다. 사회가 다양화되고 복잡해지면서 우리가 다루어야 하는 정보의 양은 더욱 늘어나게 되었고, 한편, 필요한 정보는 통신망으로 연결되어진 컴퓨터를 통하여 쉽게 얻어질 수 있게 되었다. 정보화시대 초기에는 컴퓨터란 어떠한 특수집단에 의해 특정한 장소에서만 사용되는 것으로 인식이 되었고 또 실제로 그랬으나 지금은 저렴한 중소형 컴퓨터의 대량보급과 통신기술의 발달로 여러 컴퓨터들이 통신수단을 이용하여 연결되어 서로의 정보를 공유하고 계산력(computing power)을 빌려 쓰는 추세이다. 이렇게 구성되는 컴퓨터망(computer network)은 1968년 미국방성의 ARPANET이라는 연구망을 효시로 INTERNET, BITNET, VNET, DECNET, CSNET, USNET, MILNET 등등 수많은 컴퓨터 망들이 선진국들의 자국내에 그리고 또 국제적으로 형성되어 정보교환을 용이하게 해 주고 있다.

전산망이란 용어가 컴퓨터망과 혼용되어 쓰이기도 하나 본고에서는 컴퓨터들과 컴퓨터망을 포함한 정보처리를 위해 사용되는 총체적인 분산정보시스템(Distributed Information System)의 뜻으로 전산망이란 용어를 쓰겠다. 국내에서 추진되고 있는 행정망, 금융망, 교육연구망, 국방망, 공안망의 5대 국가기간 전산망도 이러한 개념의 전산망이다. 우리나라에서도 이 전산망들이 완성되면 정보화 사회로의 도약이 급진전 할 것은 명약관화하다.

### 1.2 전산망 안전의 필요성

정보화시대가 도래함에 있어서 가장 중요한 걸림돌이 되고 있는 것은 정보를 처리하고, 저장하고, 전달하는 전산망이 얼마만큼 안전할 것인가에 대한

---

(1) 본 연구는 전산원의 전산망관리 표준화연구회 보안관리 소위원회에서 1990년에 행해졌던 연구의 결과임.

(2) 정회원, 포항공과대학 전자전기공학과
(3) 정회원, 성균관대학 정보공학과
(4) 정회원, 고려대학 전산과학과
(5) 정회원, 포항공과대학 전자계산학과

사용자의 우려이다. 그러므로 전산망의 안전에 대한 대책을 세워 사용자의 우려를 조속히 불식시키는 것이 정보화를 앞당겨 국가를 선진 대열로 이끌어 놓을 수 있는 지름길이 될 것이다.

우리는 본고에서 국가기간전산망에 닥칠 수 있는 위협요소들을 먼저 살펴보고 그 위협요소들에 대하여 어떻게 대처해야 하는가에 대해 우리들의 관점을 보여줌으로써 전산망 안전에 대한 대책을 세울 때에 도움이 되었으면 하는 바이다. 여기에서 위협이라 함은 정보의 노출이나 불법적인 변경, 파괴에 관한 것 뿐만 아니라 전산망 자체 혹은 그 일부가 피해를 입어 마땅히 받아야 할 서비스를 받지 못하는데에 대한 위협도 포함한다. 본고에서는 특히 기술적인 대책을 중심으로 세부각론보다는 전산망 전반에 걸친 안전의 문제와 대책을 총론적으로 다루었다.

## 1.3 위협요소

그림 1은 전산망의 한 모형과 각 부분에서 일어날 수 있는 위협요소들을 보여준다. 이러한 위협요소들을 분류해 본다면 아래와 같다.

### 1.3.1 자연재해와 환경으로부터의 위협

전산망은 번개, 태풍, 홍수, 지진 등 인간이 관련되지 않은 자연 재해로부터 전반적으로 위협을 받을 수가 있다. 이런 자연재해는 정전을, 특히 번개와 지진은 화재를, 태풍과 홍수는 누수를 야기시킬 수 있다. 정전은 위의 천재이외에도 발전이나 송배전상의 문제로 또는 누수에 의해서, 심

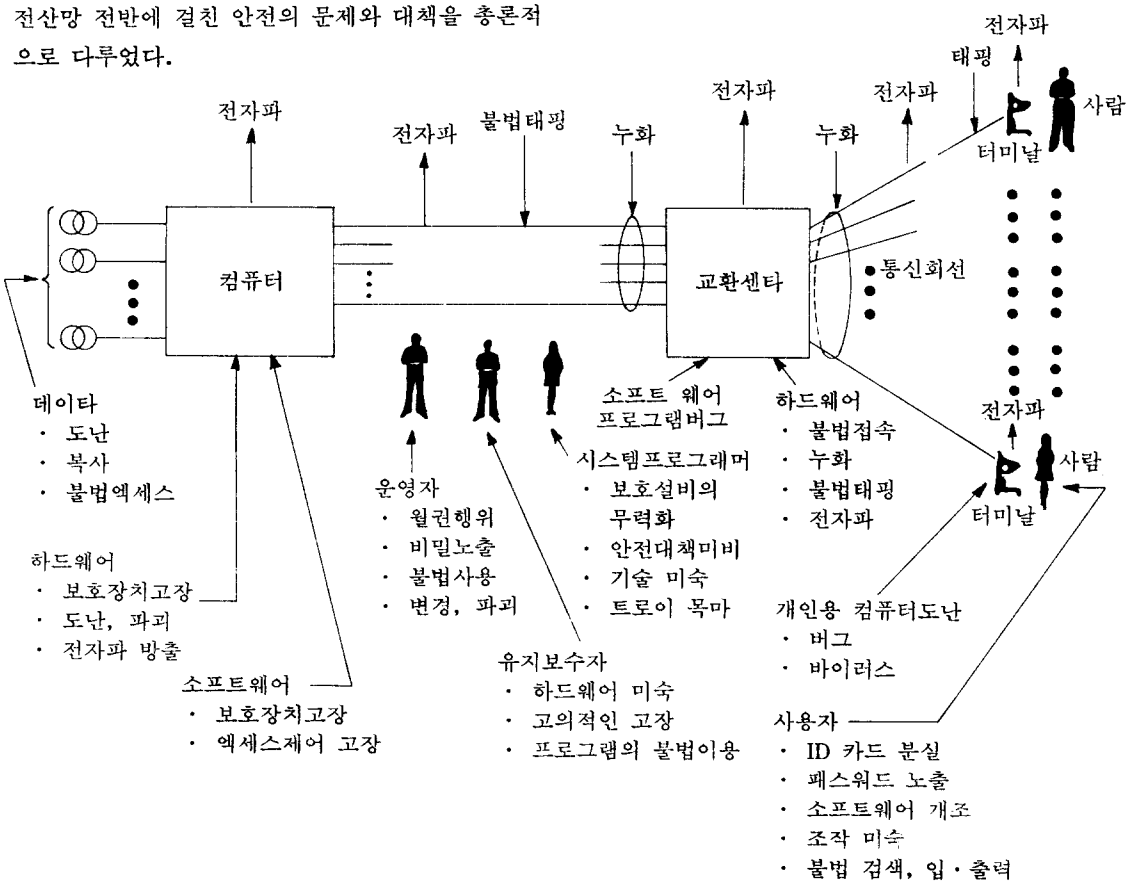



그림 1. 전산망의 위협요소들

지어는 옷에서 생기는 정전기에 의해서도 발생할 수 있으며, 정전에 의해서 작업중의 화일이 파손되거나 전송중인 데이타가 손실될 수도 있다. 화재는 정전과는 달리 시스템에 물리적으로 영구적이며 총체적인 피해를 주며, 발생요인으로는 누전, 과부하, 방화, 실화 등이 있다. 누수는 누전을 야기시켜 화재의 원인이 되기도 하며, 직접적으로 기계에 피해를 주기도 한다. 이외에도 급격한 전압의 변화나 과도전류로 인해 컴퓨터 부품이 피해를 받을 수도 있다.

### 1.3.2 인간에 의한 의도적 위협

도적이나 강도들에 의해 시설물 혹은 정보가 담겨있는 테이프, 디스켓, 자료철들이 도난당하거나 파괴당할 수 있다. 사보타지(sabotage)를 위한 폭탄 폭파, 통신선로나 전력선의 절단도 있을 수 있다. 또 정보가 기록된 서류, 디스켓, 테이프 등을 소각하거나 잘게 분쇄하여 버릴 때에 불완전하게 소각하거나 분쇄하는 경우와 부주의로 정보를 파기하지 않고 쓰레기 처리를 하는 경우에는 비인가자에게 그 정보를 노출시키는 위협이 따르는데, 이것을 스카벤징(scavenging)이라 한다.

전송중인 정보를 불법적으로 입수하기 위해 통신선로, 교환기 등에 유도결합(inductive coupling) 등의 기술로 수동적 태핑(passive wiretapping)을 할 수가 있고, 선로를 절단하거나 혹은 스위치 상자를 조작함으로써 불법적인 정보의 입수뿐 아니라 전송되는 정보를 부분적으로 없애거나 변경과 삽입 등을 마음대로 하는 능동적 태핑(active wiretapping)을 하는 위협도 있다. 흔히 광섬유는 이러한 태핑에 대해 매우 안전한 것으로 인식되고 있으나 단지 보통의 다른 선로에 비해 더 고도의 기술이 필요할 뿐이지 태핑의 위협이 없다고는 할 수 없다. 전자파를 이용하는 무선 선로의 경우에는 청취당하는 것을 찾아낼 방법이 없어 정보노출의 위협이 매우 크다 하겠으나 반면에 능동적 태핑(active wiretapping)은 불가능하다는 장점을 가진다. 그러나 선로절단과 유사한 재밍(jamming)이라는 사보타지의 위협이 있다. 그리고 통신 선로 이외에도 정보시스템의 각 부분에서 전자파로부터 발생하는 정보가 누출될 수도 있다.

스파이나 사기꾼들이 그들의 목적을 위하여 정보를 유출하려고 하는 것은 잘 알려진 위협요소 중의 하나이다. 청소년 해커(hacker)들이 재미삼아 또는 과시욕의 발현으로 행하는 각종 불법침투에 따른 정보의 유출, 파괴, 수정 등도 역시 위협한 요소 중의 하나이다. 가장 빈번한 인적 보안 파괴 행위는 시스템 내부에서 합법적으로 시스템을 사용할 수 있는 시스템 프로그래머, 컴퓨터 요원, 관리자, 보안관계자 또는 서비스 요원 등으로부터 나온다. 이는 가치있는 정보와 쉽게 접근할 수 있는 흔한 기회가 그들을 유혹하기 때문이라 분석된다.

### 1.3.3 인간에 의한 비의도적 위협

빈번한 위협중의 하나는 인간의 부주의에 의한 잘못된 데이타 입력이다. 이것은 작게는 개인 정보의 오류로 그칠 수도 있으나 전산망 자체의 큰 위협요소가 될 수도 있다. 그리고 제작시 부주의 혹은 기술부족으로 생길 수 있는 소프트웨어나 하드웨어에서의 오류(bug)가 전산망의 일부 혹은 전체의 동작을 마비시킬 수가 있다. 또한 기계를 다루는 데에 있어서의 미숙함이나 조작 실수도 흔한 안전 위협이다.

### 1.3.4 소프트웨어 위협

소프트웨어는 특정한 정보처리를 수행하기도 하고 특히 운영체제 등과 같이 전산망의 동작을 제어하는 핵심적 역할을 하기도 한다. 소프트웨어를 위협하는 것은 컴퓨터 바이러스가 가장 대표적이다. 바이러스는 일반적으로 실행형 화일(excutable file)을 찾아 감염시킴으로써 전염된다. 감염된 바이러스는 보통 어느 지정된 시간이나 지정된 조건에서 어떠한 악의적인 행동을 한다. 예를 들면, 일부 혹은 전체의 화일을 지움으로써 그 화일들로부터 행해져야 하는 컴퓨터의 동작을 마비시키기도 하고 중요한 정보를 삭제 혹은 변경시키기도 한다. 바이러스와 유사한 것으로 벌레(worm) 등의 컴퓨터 기생충(병균)들이 있는데 약간씩의 상이점이 있다. 예를 들어 벌레는 바이러스와 달리 자체가

독립된 화일로 존재하며 자체의 생명력이 있어 스스로 다른 시스템으로 전염되어 가기도 하나 피해를 주는 방식에서는 별 차이점이 없다.

이외에도 소프트웨어를 위협하는 요소는 많다. 대표적인 몇가지 예를 들면 숨겨진 소프트웨어나 하드웨어 메카니즘으로서, 개발시 개발자가 보안 절차를 우회해 시스템에 자신만이 아는 비밀침투 방법을 설치하여 피해를 입히는 트랩도어(trap-door), 정상적으로 보이는 유용한 프로그램에 몰래 트랩도어 등을 덧붙여 설치해 피해를 주는 트로이 목마, 많은 은행구좌들에서 이자 계산시 등 눈에 잘 띄지 않게 조금씩 잘라 내어 큰 이득을 취하는 샐라미 기술(salami technique), 컴퓨터의 작동이 비정상적일 때에 통상적인 보안 절차를 우회하여 컴퓨터의 작동을 정상화시키는 절차를 악용해 프로그램이나 데이타를 변경시키는 수퍼재핑(super-zapping) 등의 안전위협이 있다.

## 2. 전산망 안전 대책

정보화 시대를 앞당기기 위하여 우리는 전산망의 안전에 대한 대책을 세워 사용자의 우려를 없애주어야 하겠다. 전산망 안전대책은 기계나 정보 등과 관련된 인간외의 기술적인 대책과 그밖에 여러가지 인간과 관련된 대책으로 구별된다. 본고는 기술적인 안전대책에 중점을 둔다. 하지만 그 기술을 사용하는 주체가 사람이기 때문에 기술적인 대책만으로는 전산망의 안전이 보장될 수는 없다. 여기서 사람에 관련된 대책은 크게 두가지로 나눈다. 첫째, 부주의에 의한 안전 사고 등을 방지하는 것으로 교육 및 요원관리를 통한 대책과 둘째, 고의로 행한 안전 저해의 행위에 대한 책임을 지게 하는 법적, 제도적 안전 대책이 있다.

### 2.1 교육 및 요원 관리 대책

아무리 안전기술이 발달해도 사용하는 주체인 사람이 잘 다루지 못하면 그 기술은 아무 소용이 없게 된다. 따라서 안전기술을 사용하는 요원에 대한 교육의 중요성은 매우 크다. 안전요원을 포함한 모든 전산망 사용자에 대한 안전교육은 전산망 뿐아니라 그들 자신의 안전에도 도움을 준다.

많은 전산망 사용자들은 아직도 정보가 자산이라는 개념을 제대로 갖고 있지 않으며, 정보의 도용 등이 범죄라고 생각하지 않고 있다. 이러한 도덕적 문제는 교육을 통해 무엇이 옳고, 그른가에 대한 교육으로 해결되어야 할 것이다. 이러한 교육을 통해서 자신도 모르고 범하는 전산망의 안전을 해치는 범죄의 상당 부분을 미연에 방지하고, 전산망의 안전도를 향상시킬 수 있을 것이다.

### 2.2 법·제도 대책

교육만으로는 범죄를 막을 수 없다. 정보 보안에 관계된 법은 일반적으로 없거나 혹은 있더라도 그 강도가 매우 약하다. 범법행위를 했을 경우 그 행동에 따른 책임을 무겁게 함으로써 다른 사람에게 범죄를 저지르면 큰 벌이 따른다는 인식을 심어주는 방법으로서의 형사법은 하나의 중요한 안전대책이다.

전산망의 안전도를 높이기 위하여 필요한 조치들을 강제 규정으로 하여 지키도록 하는 것도 매우 중요한 일이다. 그 중의 하나는 여러 안전관계 제품을 만드는 기술에 관해 합당한 표준을 정하고, 그 제품들이 표준에 맞게 만들어졌는지 평가하고 승인해 주는 공식기관의 설정과 적절한 제도를 규정하는 것이다. 또 안전에 관계되는 절차들에 관해서도 표준 혹은 지침을 만들어 널리 사용하게 하고 새로 나오는 절차는 미리 검토, 승인을 받게 하며, 정해졌거나 승인된 절차들이 제대로 시행되는지 등의 감사를 하는 기관과 제도도 필요하다.

### 2.3 기술적 대책

본고의 목적은 인간 외적인 정보보호 수단으로서의 기술적 대책에 관해 총괄적으로 서술함으로써 전산망 보안의 한 분야에 대해 보다 잘 이해할 수 있도록 도와주는 것이다. 기술적 대책에 관해서는 다음 장에 보다 자세히 설명되어 있다. 그러나 앞에서도 언급되었듯이 기술적 대책 이외에도 중요한

법, 제도, 교육, 그리고 관리적인 대책들에 대해서도 많은 연구가 필요하다.

## 3. 전산망 안전 기술적 대책

전산망 안전에 대한 기술적 대책은 여러가지 관점에서 설명될 수가 있다. 3.1에서는 안전 대상별로 기술대책을 설명하고, 3.2에서는 안전 기술별로 기술대책을 설명하며, 3.3에서는 안전 서비스별로 기술대책을 설명하고자 한다.

### 3.1 안전 대상별 대책

전산망 안전 보호의 대상이 되는 것은 전산망을 구성하고 있는 모든 구성요소들이다. 각 전산망의 구성 요소 즉, 안전 대상에 따라 그 위협요소가 다르고 이에 따른 대책도 다르다. 여기에서는 각 안전 대상별로 그에 따른 대책을 살펴보고 일반적으로 해당되는 천연재해 등의 위협요소는 다루지 않는다.

#### 3.1.1 주전산기

전산망에 있어서는 주전산기(main computer) 자체가 중요한 자산일 경우가 많고 중요 정보도 주전산기 내부나 그 주위에 있는 것이 보통이다. 그러므로 물리적 안전이 가장 필요한 대상이다. 물리적 접근제어는 신원확인을 위한 통상적 절차 등의 확인방법 또는 열쇠나 카드 등의 소유에 의한 확인, 패스워드(password) 등의 지식에 의한 확인, 그리고 신체적, 행위적 특징을 측정하여 확인하는 방법(biometrics) 등이 사용된다. 스마트 카드(smart card)에 관해서는 3.2.3에서, 패스워드(password) 관리에 대해서는 3.2.2에서, 생체측정(biometrics)에 관해서는 3.2.4에서 다룬다.

정보의 처리와 보관은 운영체제에 의해 제어 받으므로 안전한 운영체제를 사용하는 것이 중요하다. 또 그 안전도를 증명하는 것도 필요하다. 이들은 3.2.7과 3.2.8에서 다룬다.

주전산기 뿐 아니라 개인용 컴퓨터(personal computer)에서도 컴퓨터 바이러스는 많은 문제를 일으키고 있다. 이 또한 중대한 안전 저해 요소이며 3.2.9에서 다룬다.

#### 3.1.2 개인용 컴퓨터

개인용 컴퓨터는 일반적으로 안전하게 보호되지 않은 장소에 방치되는 것이 보통이며, 그 사용자들도 흔히 전문가가 아니다. 또한 고가의 물리적 보안방법은 경제적인 이유로 사용되지 않는다. 개인용 컴퓨터는 그 크기가 작기 때문에 그 자체가 도난 당할 수가 있다든가, 또는 누구든지 하드 디스크나 디스켓의 화일을 보거나 수정할 수 있다는 것 등이 주전산기와 다른 점이다. 그리고 개인용 컴퓨터가 네트워크(network)에 연결되어 사용될 경우 그 컴퓨터가 보관하고 있는 주전산기의 자동 로그인(log-in)하는 절차를 도용당할 수 있다. 또한 개인용 컴퓨터는 해커(hacker)들에 의해서 전화선에 연결되어 있는 컴퓨터를 찾는 것 등의 색다른 위협요소의 도구가 될 수도 있다.

보안 대책으로서는 중요한 정보를 하드 디스크에 남기지 않고 디스켓에 넣어 안전한 장소에 보관하거나 개인용 컴퓨터 자체를 캐비넷에 넣어 보관하거나 고리(chain)로 묶어 놓는 등의 저렴한 물리적 보안을 생각할 수 있다. 또 접근 제어 소프트웨어를 설치하여 패스워드 없이는 로그인하지 못하게 하거나, 중요한 화일은 암호화하여 보호하는 등의 여러가지 방법이 있다.

#### 3.1.3 데이타베이스

데이타베이스의 사용은 근래에 와서 급증하고 있다. 여러가지 정보를 한 데이타베이스에 집중시켜 저장해 놓는 것은 편리성을 위해서는 좋지만 불법접근, 악의적인 수정 등의 위협에 대해서는 훨씬 더 위험하다. 따라서 데이타베이스의 안전을 위해서는 어떠한 사람도 불법적으로는 데이타에 접근, 변경, 그리고 삭제할 수 있어서는 안되고, 허가받지 않은 사람은 그 자료의 내용을 추론할 수 없어야 한다. 하지만 이러한 안전성을 위해 비용이 너무 많이 들거나, 저장된 데이타의 양이 지나치게 늘어나서, 합법적인 사용자가 합법적인 일을 하는데 지나치게 불편을 초래해서는 안된다.

불법적으로 데이타에 접근하는 것을 방지하는

것을 접근제어(access control)라고 한다. 이를 위해 먼저 접근하고자 하는 사람이 누군가를 알아내는 식별(identification)과 그리고 식별된 사람이 정말로 그 사람인지를 인증(authentication)하는 과정이 필요하다. 또한 보호되어야 할 데이타와 그 데이타를 사용하고자 하는 사람 사이의 관계를 매트릭스(matrix)로 나타내어 누가 어떤 데이타에 무슨 권한을 갖고 있는지를 정해 놓고 거기에 따라 접근시 행동을 제어하는 방법이 있다.

데이타의 암호화는 데이타를 보호하는 한 방법이 될 수 있다. 그러나 데이타를 저장시킬 때와 다시 추출할 때까지의 시간적 간격이 큰 경우에는 그 동안의 키를 안전하게 관리하는 것이 매우 어렵게 된다.

정보를 비밀의 정도에 따라 등급을 부여하여 그 등급에 적합한 보호조치를 하는 것이 필요하다. 등급을 나누는 방법은 나라마다 또 기관마다 다르나 정보에 등급을 부여할 때 너무 낮게 주어도 비밀유지에 문제가 발생하기 때문에 좋지 않고, 또 너무 높게 주어도 접근이 필요 이상으로 통제되므로 좋지 않다.

### 3.1.4 네트워크

두개 이상의 컴퓨터 혹은 다른 정보 사용 요소(혹은 시스템)들이 통신선로와 교환설비를 통해 연결되어 서로의 정보를 이용할 수 있게 하는 통신시스템을 네트워크라 한다. 근거리 통신망(LAN)과 같은 소규모 네트워크로부터 전 지구를 거쳐 수만개의 컴퓨터가 연결된 대규모 네트워크도 있다.

IBM의 SNA(Systems Network Architecture)와 Honeywell의 DSA(Distributed Systems Architecture) 등과 같이 어떤 회사가 자사의 제품들을 연결하는 네트워크나 여러 회사 제품을 구별없이 연결한 개방 네트워크는 각각 안전 위협요소가 다르며 그에 따른 대처방안도 각가 다르다. 특히 ISO(International Standard Organization)는 OSI(Open Systems Interconnection)의 7계층 구조를 표준화하고 있으며, 거기에 따른 안전 위협 및 대책에 관한 연구가 많이 진행되고 있다(예 : ISO 7498.2 OSI 참조모델 보안구조-Security Architecture).

근거리통신망은 그 나름대로 또 다른 안전문제를 가지고 있으며, 그의 안전에 관해서는 IEEE의 802.10분과에서 이에 필요한 보안 표준을 연구하고 있다.

### 3.1.5 통신 선로

전송중인 정보의 불법적인 입수를 위해 동선으로 된 통신선로에 유도 결합 등의 수동적 태핑(passive wiretapping)을 하거나 선로에 불법기기를 연결하는 것은 선로상의 임피던스(inpedance)를 자주 측정하여 그 변화를 감지함으로써 찾아낼 수 있다.

광섬유에 대한 태핑 역시 광 강도의 급격한 변화를 알아 냄으로써 찾아낼 수 있다. 전자파를 이용하는 무선 선로에 있어서 청취만을 할 경우 찾아낼 방법이 없으나 불법 전파송신은 비교적 쉽게 찾아낼 수 있다. 재밍(jamming)이라는 전파방해 위협의 경우에 있어서는 반재밍(antijamming)이라는 방법을 쓰기도 한다.

### 3.1.6 분산정보처리

분산정보처리에는 주전산기, 데이타베이스, 소프트웨어, 네트워크 통신선로 등 여러가지 요소들이 포함된다. 따라서 이들 각각의 대상에 따른 안전조치가 필요하며 이들이 유기적으로 결합하였을 때 발생할지도 모르는 안전상의 모든 요소에서 동등한 수준으로 이루어져야 된다는 점이다. 요소별로 안전 수준이 서로 다른 경우, 시스템의 안전은 최저수준 요소의 안전수준으로 되며, 이러한 경우 상위수준의 안전을 유지하는 요소는 비용의 낭비내지는 시스템 오버헤드를 초래하는 결과가 된다.

### 3.1.7 소프트웨어

소프트웨어는 크게 시스템 소프트웨어와 응용 소프트웨어로 구분할 수 있는데 안전대상으로서의 소프트웨어는 양쪽 모두 앞에서 언급된 데이타베이스와 유사한 성격을 갖는다. 따라서 안전에 대응하는 방법도 데이타베이스에 적용되었던 것들을 그대로 적용할 수 있다. 그러나 소프트웨어의 경우는 그 안전이 침해 당했을 경우 피해의 범위가

넓고 침해 사실의 발견이 어려워 피해의 지속 시간이 길어지게 될 가능성이 크다. 특히 시스템 소프트웨어의 침해는 그 시스템 소프트웨어를 이용하는 모든 이용자에게 광범위한 피해를 줄 수 있어 그 안전관리에 소홀히 해서는 안된다.

소프트웨어가 불법 변조되었을 경우, 그 발견이 용이하지 않으므로 변조를 위한 접근이 불가능하도록 철저한 물리적 접근제어는 물론 시스템 내부에서 불법 변조에 대응하기 위한 기술적 장치 또한 마련되어야 한다. 예를 들면 소프트웨어의 불법변조를 막기 위해 원시코드(source code) 저장시 암호화 기법이 사용될 수 있다.

3.1.8 문서

종이 서류로 된 문서 역시 전산망의 일부이다. 흔히 처리된 정보는 그 결과가 프린트된다. 그 프린트물을 안전하게 보관하고, 철저하게 파기하는 것은 거기에 쓰여진 정보 뿐만 아니라 전산망의 안전에 대한 노출을 방지하는 것이다. 특히 일반 정보 보다도 전산망 안전에 있어서 문서의 취급에 관한 보안대책은 더욱 주의를 기울여야 한다.

## 3.2 안전 기술별 대책

어떠한 대상을 위해 어떠한 서비스를 할 때 거기에 알맞는 필요한 도구들이 있다. 여기에서는 안전을 이룩하기 위해 필요한 도구 즉, 기술들에 관하여 설명한다.

3.2.1 위험(Risk) 분석

전산망 안전을 위해 가장 먼저 행해져야 할 것은 전산망의 안전에 어떠한 위협요소가 있는가 어떠한 취약점들이 있는가, 그리고 그 위협요소와 취약점들에 의해 어떠한 손실이 있을 수 있는가에 대한 위험(risk) 분석이다. 위험분석은 전산망 전체적으로는 할 수 없는 것이 보통이고 각 업무부분, 지역, 대상, 시점 등으로 세분하여 행해져야 한다. 이를 위해서 팀이 구성되어야 하는데 그 구성원으로는 위험분석의 전문가 뿐만 아니라 그 지역의 현상과 업무를 잘 아는 실무자들도 같이 포함되어야 한다.

위험분석 기술은 물론이고, 위험분석에 따른 대책을 세움에 있어서 관련 기술도 중요하지만 이와 더불어 일종의 교육과 제도도 꼭 필요하다. 대책 중 우선 손쉬운 것은 간단하면서도 안전에 중요한 것을 검사목록(check list)으로 만들어서 그 검사목록에 따라 안전 점검을 생활화하는 것이다.

3.2.2 패스워드(Password) 관리

접근제어(access control)를 하기 위해서는 신원확인이 일차적으로 행해져야 한다. 이 때 가장 흔히 쓰이는 것은 그 신원 확인 대상자 혼자만이 알고 있는 사항을 확인하는 것이다. 혼자만의 지식이 패스워드가 되어 어떠한 장소나 정보에 접근 가능하게 한다. 이 패스워드를 어떻게 관리하는가도 역시 중요한 문제이다. 한국전산원의 전산망 관리 표준화연구회의 보안관리 소위원회에서는 1990년 12월에 패스워드 사용지침(안)을 내놓았다. 그리고 같은 내용을 통신정보보호학회지 창간호 pp.109~118에 "패스워드 시스템의 보안에 관한 고찰"이라는 제목으로 게재하였다. 이 패스워드 시스템의 보안에 관한 연구결과는 전산망의 사용자(end-user) 관리를 담당하고 있는 보안 담당자들에게 큰 도움이 될 것이다.

3.2.3 스마트 카드(Smart Card)

신원을 확인할 때에 그 신원확인의 대상자 혼자만 가지고 있는 물건으로 확인할 수도 있다. 열쇠, 꼬리표(Tag), 카드, 토큰 등이 그 예이다. 물론 이러한 것들은 신원확인 대상자마다 각기 달라야 한다. 열쇠와 같이 물리적인 구별을 할 수 있는 것도 오래 사용되어 왔지만, 근래에 들어서 스마트 카드와 같이 전자적으로 구별이 가능한 방법이 널리 사용되고 있다. 흔히 쓰이고 있는 카드로는 자기식 카드(magnetic stripe card)로서 공중전화카드, 은행 신용카드(credit card) 등이 있고, 이것은 건물 혹은 방의 출입용이 실제로 많이 쓰인다. 그러나 이런 자기식 카드는 남에게 그 카드 안에 들어있는 신원 확인용 정보가 쉽게 누출될 수 있기 때문에 안전도가 그리 높지 못하다.

근래에 들어서 일반 자기식 카드와 같은 크기의

카드에 반도체 기억장치(IC-chip)를 집어 넣어 IC의 메모리에 많은 정보를 저장할 뿐 아니라, IC 속의 중앙처리장치(CPU)가 패스워드를 확인하는 경우에만 메모리의 일부를 보여주는 등의 기술로서 메모리를 보호, 처리하는 개념이 실용화되어 프랑스를 선두로 여러 선진국에서 쓰이고 있다. 이렇게 중앙처리장치(CPU)가 포함된 IC 칩을 집어 넣은 카드를 스마트 카드(smart card)라 한다. 스마트 카드는 일반적으로 카드 표면 한쪽에 있는 전기적 접점(electric contact)을 통해 외부와 통신을 한다. 이렇게 중앙처리장치(CPU), 메모리, 통신용 단자가 있으므로 스마트 카드는 주머니에 들어가는 궁극적인 개인용 컴퓨터(ultimate personal computer)라 부르기도 한다. 중앙처리장치(CPU)가 없이 메모리 칩만 들어있는 카드는 스마트 카드라 하지 않고 메모리 카드라고 한다. 스마트 칩이 들어간 카드 이외에 열쇠나 꼬리표 같은 다른 형태를 갖는 스마트 토큰도 사용되고 있다.

스마트 카드는 일종의 개인용 컴퓨터라고 생각할 수 있으므로 접근 통제 뿐만 아니라 은행, 백화점, 여행사 업무, 개인용 수첩, 의료용 등 헤아릴 수 없는 응용분야에서 제시되어 실제로 그 응용이 실현되고 있다. 국제표준화기구(ISO)에서는 스마트 카드의 형태와 금융업무 등에서의 사용 절차에 관해 표준화 활동을 해오고 있다.

### 3.2.4 생체측정(Biometrics)

신원을 확인할 때에 그 신원 확인 대상자 혼자만의 특징으로 확인할 수도 있다. 우리가 흔히 쓰는 신분증에 붙어 있는 사진은 사진과 얼굴을 비교해 봄으로써, 또는 서명은 종래부터 보아왔던 서명과 같은 가를 확인하는 것과 같다.

사람의 특징은 신체적인 특징과 행위적인 특징으로 구분할 수 있다. 사람의 특징은 시간과 환경에 따라서 변하기도 한다. 그러므로 어떠한 특징이 어느 특정인에게 속한 것인가를 판별할 때에 두가지 오류를 범할 수 있다. 첫째, 그 특정인의 특징이 원래 소유자의 것이 아니라고 하는 오류로서 합법적인 사용자가 마땅히 받아야할 시스템의 서비스를 받지 못하게 하는 불편을 준다. 둘째, 제 3 자의 특징을 그 특정인의 것이라고 잘못 판별하는 오류로서 안전에 직접적인 위협이 된다. 넓은 의미에서의 안전도를 높이기 위해서는 앞의 두가지 오류가 모두 작아야 되지만 어느 한가지 신체적이나 행위적인 특징을 비교하는 방법을 고정하여 쓰는 경우 판정치 기준을 정하기에 따라 어느 한쪽의 오류는 다른 한쪽의 오류를 늘림으로서만 줄일 수 있다. 따라서 그 기준을 정하는 것은 위험분석의 결과에 따라야 한다. 두 타입간에 오류에 대한 합의 최소치가 안전도의 판단 기준으로 쓰이기도 한다.

전산망의 안전을 위해 쓰일 수 있는 신체적, 행위적 특징들은 안전도가 높아야 하고 쉽게 전기신호로 바꿀 수 있어야 한다. 즉, 생체측정은 많은 특징을 가져야 하며 그 특징을 빠르고 저렴한 가격으로 찾아내어 다른 사람들의 특징과 비교할 수 있어야 한다. 정확한 것으로는 지문인식, 눈 망막의 실핏줄 무늬, 그리고 DNA 등이 있으나 일반적으로 이러한 것들은 가격이 비싸다. 그리고 손으로 서명을 할 때 특수 펜과 판을 사용함으로써 서명시 펜 끝의 센서에 측정되는 펜의 압력과 가속도로부터 특징을 찾아내는 방법도 사용되고 있고, 성문(voice signature)이라고 불리우는 목소리의 역동적인 특수성을 찾아내어 비교하는 법, 얼굴이나 손의 모양에서 특징을 찾아내는 법도 연구 실용화되고 있다. 타자기를 칠 때나 전화기 번호판을 누를 때의 리듬(keystroke dynamics)을 구별하여 사용하기도 한다. 행위적 특징을 사용하는 경우 시스템을 학습시키는 과정이 필요하다.

### 3.2.6 물리적 안전

번개, 태풍, 홍수, 지진 등의 천재를 막는 것은 전산망에 있어서도 일반적인 경우와 특별히 다르지 않다. 그러나 이들로부터 야기되는 이차적 피해인 화재, 누수, 정전에 대한 대책은 전산망이란 특수성을 고려하여야 한다.

화재의 감지 역시 일반 건물의 경우와 같이 빠르고 정확할 수록 좋으나 화재 진압시 컴퓨터나 교환기등이 물과 어떤 화학약품에는 약하므로 할론(Halon)가스 혹은 이산화탄소($CO_2$)가스 등을 사용하는 것이 좋다. 물이나 기계에 해로운 화학물

질의 사용은 위험부담이 크므로 부득이한 경우가 아니면 피하는 것이 좋다.

누수나 지나친 습기는 누전을 야기시켜 화재의 원인이 되기도 하며, 직접적으로 금속 표면의 부식이나 반도체를 손상시키는 피해를 주기도 한다. 습기를 감지하여 건습제로 습도조절을 하거나, 천정의 수도관 파열이나 화재시 물로 진압하게 될 경우 플라스틱 커버를 자동적으로 씌우는 장치를 사용하는 것도 필요하다. 따라서 기계를 바닥으로부터 높게 설치해야 한다.

정전, 급격한 전압의 변화 또는 과도전류로부터 작업중 화일의 파손, 전송중인 데이타의 손실 그리고 컴퓨터 부품파괴 등의 피해를 받을 수 있다. 무정전 전원 공급장치 UPS(Uninterruptible Power System)와 자체의 임시 발전기를 구비하여 정전을 대비하며, 전압조정기(voltage regulator), 라인 필터(line filter) 등으로 급격한 전압이나 전류의 변동을 막아야 한다.

3.2.6 물리적 안전

도둑이나 강도들의 침입자를 사전에 감지하고 방지하는 것이 물리적 보안의 가장 중요한 요소이다. 빛, 소리, 열, 진동, 압력, 커패시턴스(capacitance), 고주파(microwave), 에너지 비임 등의 갑작스러운 변동을 감지함으로써 경보기를 울린다거나 자동으로 방어시스템을 가동시킨다. 경비원, 경비견, 레이다, 폐쇄회로텔레비젼(CCTV) 등을 사용한 적극적인 감지방법도 있다. 다른 것들과 마찬가지로 감지방법도 두가지 이상의 방법으로 다중화하는 것이 좋다. 침입방지에는 위장시설, 높고 튼튼한 울타리, 경비원과 경비견, 기계적 혹은 전자적 잠금, 레이저나 고압전기 등의 방법들이 있다.

3.2.7 안전 운영체제 커널(Kernel)

운영체제에 의해서 관리되는 데이타나 다른 자원들의 가치에 적합한 보호수준을 제공하기 위해 하드웨어나 소프트웨어의 기능들을 효과적으로 조정하는 운영체제(OS)를 안전 운영체제라 부른다. 이 안전 운영체제에서 가장 중요한 것은 안전 커널(security kernel)인데, 이는 하드웨어와 소프트웨어로 구성되어, 지역화된 기능으로서 사용자와 자원의 액세스를 관리하는 것이다. 여기서 어떤 주체가 객체를 액세스하는 모든 과정을 중재하는 참조 모니터(reference monitor)의 개념이 활용된다.

3.2.8 공식 검증(Formal Verification)

공식 검증(formal verification)은 컴퓨터 시스템의 공식 명세(formal specification)와 공식 안전 정책 모델(formal security policy model)이 일치하는가를 수학적 증명을 하듯이 증명하는 것이다. 안전 정책(security policy)이란 한 기관이 어떻게 민감한 정보를 관리, 보호, 분배하는가를 정한 법, 규칙 등의 집합을 말한다. 공식 안전 정책 모델이란 안전 정책을 수학적으로 상세히 서술한 것이다. 좀 더 자세히 말하자면 이 모델은 시스템의 초기상태와 시스템이 한 상태에서 다른 상태로 옮겨가는 과정과 그 시스템의 안전한 상태를 정의하고 서술한 것이다. 이런 모델 중 대표적인 것으로 접근제어 규칙(access control rule) 등을 기술한 공식 전이 모델(formal transition model)인 벨 라파둘라 모델(Bell-Lapadula Model)이 있다.

이러한 공식 검증은 일명 오렌지 북(Orange Book)이라고도 불리는 미 국방성에서 발행된 TCSEC(Trusted Computer System Evaluation Criteria)라는 책에 의해 분류된 여러 사용자가 이용하는 독립된 컴퓨터의 안전도 분류 중에서 가장 상위 분류에 해당하는 분류 A의 요구조건이다. TCSEC의 분류에 의하면 분류 D는 아무 안전 장치가 없는 시스템을 말하고, 분류 C는 자발적인 방어(discretionary protection), 분류 B는 강제적인 방어(mandatory, portection)의 제어수단을 갖는다. A, B, C의 구분은 더 세분화되어 A2, A1, B3, B2, B1, C2, C1의 등급으로 안전도가 높은 순서부터 분류된다.

3.2.9 컴퓨터 바이러스 검출(Detection)과 치료(Cure)

컴퓨터 바이러스를 막고, 찾아내고, 치료하는 것은 실제 병균인 바이러스와 의료진과의 끊임없는

전쟁과도 같다. 바이러스에 대한 백신이 나오면 새로운 바이러스가 나오고 또 새로운 치료제가 나오고 하는 과정이 반복된다. 이렇게 치료제를 사용하는 것은 이미 알려진 바이러스를 치료하는 데에는 유용하나 새로운 바이러스에 대해서는 효과가 없다. 백업을 자주하는 방법, 가상 메모리를 이용하는 방법, 공개 키 암호 시스템의 디지탈 서명을 이용하는 방법 등이 고려되어야 한다.

3.2.10 암호학

암호학은 2000년전 로마의 시저(Caesar) 당시부터 비교적 최근까지 정보의 안전한 전달을 위하여 주로 정부나 군에 의하여 사용되어 왔다. 암호학의 개념은 암호화에 사용되는 알고리즘과 장비의 일체는 공개되는 반면, 키라고 불리는 알고리즘의 중요한 부분을 감춤으로써 정보의 비밀성이 유지되는 것이다. 알고리즘에는 크게 키가 정보를 보내는(암호화하는) 사람과 받는(복호화하는) 사람이 사용하는 키의 상이 여부에 따라 단일 키 암호시스템(one-key cryptosystem)과 이중 키 암호시스템(two-key cryptosystem)으로 구분된다.

단일 키 암호시스템은 보내는 쪽과 받는 쪽이 동일한 키를 사용함으로써 모두 감추어야 하므로 다른 이름으로 비밀키 암호시스템(secre-key cryptosystem, symmetric cryptosystem)이라고도 불린다. 반면 이중 키 암호시스템은 한쪽 키를 밝혀도 다른 쪽 키는 물론 암호화 된 내용도 밝혀지지 않으므로 한쪽 키를 공개시켜도 된다. 그래서 이를 공개 키 암호시스템(public-key cryptosystem, asymmetric cryptosystem)이라 부르기도 한다. 이 공개 키 암호시스템은 전달되는 정보의 보호 뿐 아니라 디지탈 서명, 인증, 내용확인, 부인 봉쇄 등의 전산망 보안의 새로운 응용분야를 창출해 냄으로써 암호학이라는 새 학문분야를 열었다. 워낙 새로운 학문이라 제일 처음 생긴 학회의 역사도 10년이 지나지 않으나 암호학은 눈부시게 빠른 속도로 발전해 왔고 또 발전할 것이다. 우리나라는 이제야 학회가 결성됐고, 소수의 정부관계 연구기관에서만 연구가 활성화되고 있을 뿐이다. 정보화시대에 필수불가결한 암호학에 전념할 많은 연구 인력이 절실히 요구되고 있는 현황이다.

3.2.10.1 비밀 키 암호방식

비밀 키 암호방식은 정보를 암호화할 때와 복호화할 때 같은 키를 사용하는 알고리즘을 이용하는 방식으로 모든 키는 비밀을 유지해야 한다. 공개 키 암호방식이 나오기 전까지의 모든 암호시스템은 이 방식을 이용해 왔고, 아직도 암호시스템의 주종을 이루고 있는 암호방식이며, 그런 의미에서 이를 관용 암호방식이라고도 부른다.

통신과 컴퓨터가 발달하기 전까지 이 비밀 키 암호방식은 주로 정치, 군사, 외교의 목적으로 사용되어 왔으나 근래에는 금융, 기업 개인에 이르기까지 널리 사용되고 있다.

비밀 키 암호방식을 위한 알고리즘의 종류에는 데이타를 취급하는 단위의 크기에 따라 데이타를 큰 블럭(block)으로 나누어 현재의 출력블럭은 현재의 입력블럭에만 영향을 받는 블럭 사이퍼(block cipher)와 비트나 바이트 같이 데이타의 작은 단위를 입력으로 하며 현재의 입력에 대한 출력은 과거의 입력에도 영향을 받는 스트림 사이퍼(stream cipher)로 크게 나눈다. 위치 교환, 대치 등 단순한 방법의 블럭 사이퍼 방식으로부터 그들을 결합하여 보다 안전성을 높인 프로덕트 사이퍼(product cipher) 방식이 있다. 이 프로덕트 사이퍼 형태의 대표적인 알고리즘은 1977년 공표된 DES (Data Encryption Standard)이다. DES는 UNIX 운영체제의 패스워드를 암호화하는 "crypt"에 이용되며 특히 미국과 유럽의 은행에 의해 EFT(Electronic Fund Transfer)시스템에 이용되는 등 널리 사용되고 있다.

비밀 키 암호방식을 이용하여 통신을 하기 위해서는 쌍방이 모두 같은 키를 가져야 하므로 키의 교환이 선행되어야 한다. 따라서 새로운 사람과 통신하고자 할 때는 키가 전달되어야 하는데 그 과정의 보안이 힘들고 키의 보관 역시 어려운 면이 있다. 그럼에도 불구하고 공개 키 알고리즘에 비교하여 훨씬 알고리즘이 간단하므로 암호화하는 속도가 월등히 빠르고 소프트웨어로 구성시 화일의 크기가 작고, 하드웨어로 구성시 회로가 간단해

지는 경제적인 이유로 널리 이용되고 있다.

3.2.10.2 키 관리

암호시스템의 안전은 암호 알고리즘의 안전도에 의존하지만 암호 알고리즘이 아무리 완벽하다고 해도 그 키가 노출된다면 아무 소용이 없다. 암호학적 키의 발생, 분배, 보관 그리고 파기에 이르기까지의 모든 과정을 키 관리라고 부른다.

암호학적 키의 발생에 있어서는 타인이 예측할 수 없어야 하고 키가 가질 수 있는 값의 전 범위 안에서 골고루 발생되어야 하고 외부로부터의 영향을 받지 않아야 하며, 키의 발생 결과 노출이 없어야 한다. 키 생성에는 저항에서의 잡음 등 자연적인 우연성, 키 소유주가 임의로 치는 반우연적인 키보드의 입력 혹은 동전이나 주사위 던짐의 결과 그리고 키 생성 당시의 시각, 통신중인 신호 혹은 저장중인 화일 정보 등의 여러가지 요소들로부터 안전성이 검증된 키 생성 장치를 사용하여 합당한 절차를 거쳐 만들어야 한다. 이상과 같이 안전한 장치와 과정, 여러가지 우연성과 다양성 그리고 불규칙성을 이용한 암호학적 키의 생성은 많은 시간과 노력과 장비가 든다. 그래서 이러한 키는 보통 매스터 키 혹은 터미널 키로만 쓰이고 터미널 사이의 한 통화 사이에만 쓰는 경우에는 따로 통화 키를 사용한다. 이 통화 키는 일반적으로 터미널 키와 조금씩 다른 여러 입력으로부터 생기는 암호 모듈을 사용하여 생성시킨다.

암호학적 키의 분배에는 그 키가 매스터 키인지 혹은 터미널 키인지 아니면 통화 키인지에 따라 그 방식에 큰 차이가 난다. 매스터 키나 터미널 키의 경우, 그 중요성 때문에 분배 혹은 전송시 특별한 주의가 필요하다. 특히 전자통신 이외의 다른 방법 즉, 등기우편이나 전령 등은 특별히 고용된 사람을 통해서 전달하는 것이 필요하고 반드시 두가지 이상의 방법으로 두번 이상 전달함으로써 위험부담을 줄이는 것이 필요하다. 통화 키의 전달은 매스터 키나 터미널 키의 경우와 달리 중요성도 덜 하고 자주 바뀌어야 하기 때문에 전자통신의 방법을 사용하여 보통 매스터 키나 터미널 키로 통화 키를 암호화하여 보낸다.

암호학적 키는 파기될 때까지 안전한 장소에 안전하게 보관되어야 한다. 특히 전자적으로 보관된 경우, 정전이 되었을 때에도 안전할 수 있게 보관되어야 한다. 사람의 손에 의해 보관되고 사용되는 경우, 반드시 두명 이상의 관리 요원으로 하여금 처리하게 하는 것이 좋다.

암호학적 키 파기는 수명이 다된 키를 더 이상 사용할 수 없도록 없애는 것이다. 통화 키의 경우는 한 통화의 종료와 더불어 통화 키가 들어있던 기억소자의 부분을 다른 일정한 내용을 대치시킴으로써 파기할 수 있다. 매스터 키나 터미널 키의 경우, 파기자는 입회자가 보는데에서 키의 어느 한 부분도 재생시킬 수 없도록 파기한다.

이러한 키 관리를 포함하여 감사업무까지 대행해 주는 기관이 필요하다. 이를 키 관리 센타라 부르며 이 센타는 시스템의 가입사용자들로부터 신뢰를 받아야만 된다. 특히 비밀 키를 사용하는 시스템의 경우 이 키 관리 센타는 사용자들간의 모든 통화를 해독할 수 있기 때문에 매우 중요하다.

3.2.10.3 공개 키 암호방식

1976년 Diffie와 Hellman은 두개의 키를 이용하는 새로운 암호 시스템의 개념을 제안했다. 이는 두개의 키를 만들어서 하나만 비밀을 유지하고 다른 하나는 공개하는 방식으로 공개 키 암호방식이라 불리우며 암호 키란 모두 비밀을 유지해야 한다는 기존의 관념을 깨뜨렸다. 그들이 제안한 방식은 다음과 같은 세가지 조건을 만족해야 한다.

첫째, 암호키와 복호키를 만들었을 때 메시지를 암호화한 것을 복호화하면 원래의 메시지가 나와야 한다.

둘째, 암호 키가 주어져도 복호 키를 유추해 내기가 거의 불가능해야 한다.

셋째, 선택된 평문과 그것을 암호화한 암호문을 함께 가져도 그것들로부터 암호키를 알아낼 수 없어야 한다.

Diffie와 Hellman은 이러한 개념을 고안해 냈지만 실제로 그 조건을 만족하는 알고리즘은 찾지 못하였다. 세 조건을 만족하는 대표적인 알고리즘으로 1978년 Rivest 등이 발견한 RSA 방식이 가장 많이

사용되고 있다. 이는 큰 정수의 인수분해가 지극히 어렵다는 특성을 이용한 것이다. 그 외에도 ElGamal이 제안한 이산형 대수(discrete logarithm) 문제가 어렵다는 점을 이용한 암호방식, 크기가 다른 짐(sack)들을 정해진 크기의 배낭에 빈틈없이 채워넣는 것이 어렵다는 성질을 이용한 냅색(knapsack) 암호방식, 일반적인 오류(error) 정정부호를 복호화(decoding)하는 것이 어렵다는 점을 이용한 McEliece 암호방식 등이 있다.

공개 키 암호방식은 한개의 키를 누구에게나 알려주어도 무방하므로 공개적으로 전달하거나 전화번호부 같은 키 디렉토리(key directory)를 통해서 키를 알 수도 있으므로 비밀 키 암호방식처럼 통신을 할 때 비밀리 키를 전달할 필요가 없으므로 필요한 키의 수도 줄어들 뿐더러 키 관리의 보안 문제가 쉬워진다. 또한 어떤 공개 암호방식은 다음에 설명할 디지탈 서명(digital signature)같은 비밀 키 암호방식에서 볼 수 없는 기능을 가지고 있다. 그러나 사용하는 키의 크기가 크고 알고리즘이 복잡하여 실행 속도가 느리고 구현하기 힘들다는 단점이 있다.

3.2.10.4 디지탈 서명

서명(signature)이란 원래 문서상에 자신의 행위를 증명하기 위해 이름을 써넣는 것으로 계약 등을 할 때 이용된다. 디지탈 서명이란 문서상에서 이루어지던 서명을 전자적으로 행하는 것을 말하며 보통 문서상의 서명과 마찬가지로 송신자는 나중에 자신이 메시지를 보냈음을 부인할 수 없다.

디지탈 서명은 RSA나 ElGamal과 같은 공개 키 암호방식을 이용하여 어떤 사람 "갑"이 자신의 비밀키로 암호화 한 내용을 어느 누구든 다른 사람이 "갑"의 공개 키로 복호화하게 함으로써 그 내용이 "갑"이 직접 서명했다는 것을 확인할 수 있게 하는 것이다. 이것은 "갑"의 비밀 키는 다른 누구도 가질 수 없다는 데에 근거를 하고 있다.

또 최근 80년대 후반에 Fiat와 Shamir에 의해 소개된 자신의 정보를 상대에게 알려주지 않고 상대방에게 자신이 그 정보를 갖고 있다는 확신을 주는 영의 지식(zero-knowledge) 프로토콜의 개념을 확장하여 신원확인과 디지탈 서명을 하는 방법도 있다. 이 방법은 공개 키 암호방식보다 계산 수행이 간단한 장점이 있는 반면 키 크기와 통신량 증가 등의 단점이 있다.

이러한 디지탈 서명의 응용으로서는 3.3절에서 소개할 정보의 안전 서비스들 중 인증, 무결성, 부인 봉쇄, 컴퓨터 보안 감사 등이 있다.

3.2.10.5 암호학적 프로토콜

암호 알고리즘이 아무리 훌륭하다 해도 그 알고리즘을 사용하는 프로토콜이 제대로 되어 있지 못하면 그 시스템이나 서비스의 안전은 보장되지 못한다. 그 한 예로 떨어진 장소에서 합의된 사항에다 쌍방에서 디지탈 서명을 하게 될 경우, 한 쪽이 서명을 한 것을 받은 후 다른 쪽에서 실제로는 서명을 하지 않고서는 상대방의 서명이 포함된 전자문서를 갖지 못하게 할 수 있다. 또 신원의 인증을 할 경우, 누군가 믿을 만한 사람이 있어 그 사람이 보증을 해주는 것으로 인증을 할 수 있는데 직접 믿을만한 사람이 보증을 못할 경우, 믿을만한 사람이 보증하는 어떤 사람이 그 문제의 사람을 보증함으로써 인증을 하는 수도 있다. 이와 같이 믿음의 관계를 설정함에 있어서도 암호학적인 프로토콜이 중요한 역할을 한다. 일반적으로 암호학적인 프로토콜은 안전 서비스 그리고 안전 시스템을 구성하는 데에 있어 중요한 한 요소이다.

(다음 號에 계속)

## 참 고 문 헌

1. 타임-라이프 북스 편집부, 컴퓨터의 세계, 컴퓨터의 보안, 한국일보 타임-라이프 편집부, '90. 3.

2. 김세헌, 정보통신망의 정보보안체계 설계에 대한 종합적 연구, 한국경영과학회 '89전기통신학술연구과제 최종보고서, '90. 1.

3. 김동용, 컴퓨터 망의 보안에 관한 연구, 한국통신학회, '89 전기통신 학술연구과제 최종보고서, '89. 12.

4. International Standard Organization, "Informa-

tion Processing-OSI Reference Model-Part 2, Security architecture", International Standard ISO 7498-2, Geneva, 1988.

5. CCITT, "OSI-The Directory-Authentication framework", Recommendation X. 509, Melbourne, 1988.

6. R.R. Moeller, Computer Audit, Control and Security, Wiley, 1989.

7. J.M. Carrol, Computer Security, 2nd ed., Butterworths, 1987.

8. J.W. Wack & L. J. Camahan, Computer Viruses and Related Threats, A Management Guide, NIST Special Publication 500-166. Aug. 1989.

9. M.E. Haykin & R. B. Warnar, Smartcard Technology, New Methods for Computer Access Control, NIST Special Publication 500-157, Sept. 1983.

10. IEEE, Standard for Interoperable LAN Security, P802-10, May, 1990.

11. X/Open, X/Open Security Guide, Prentice Hall, 1989.

12. K.E. Kirkpatrick, "Standards for Network Security", Proc. of 11th NCSC, Oct. 1988.

13. Y. LeRoux, "Technical Criteria for Security Evaluation of Information Technology Product", IFIPS TC-11 Conference, May, 1990.

14. NIST, SDNS Network, Transport, and Message Security Protocols, NIST IR 90-4250, Feb. 1990.

15. 박태규, 이형수, 신종태, "컴퓨터/네트워크 시스템 보안 표준화 동향 분석", 제 2 회 정보보호와 암호에 관한 워크샵 논문집. pp.95-113, 유성, 1990. 9.

16. 한국전자통신연구소, 정보보호체계 구성 방식 연구, 1990. 3.

17. Department of Defence, Trusted Computer System Evaluation Criteria, US Government Printing Office, CSC-STD-001-83, Aug. 1983.

18. NBS, Guidelines for Automatic Data Processing Physical Security and Risk Management, FIPS Pub 31, June 1974.

19. D.E. Denning, Cryptography and Data Security, Addison-Wesley, 1982.

20. D.D. Steinauer, Security fo Personal Computer Systems, A Management Guide, BNS Special Pub 500-120, Jan 1985.

21. NCSC, Personal Computer Security Considerations, NCSC-WA-002-85, 1985.

22. European Computer Manufacturers Association, Security in Open Systems, A Security Framework, ECMA TR/46, July, 1988.

23. American National Standard for Personal Identification Number(PIN) Management and Security, ANSI X. 9.8., Jan. 1982.

24. ISO, User Requirements on Security, ISO ITS1 /SC18N2003, E.J. Humphreys, CEN/CENELEC-Toward a Taxanomy for Standardization of Security, British Telecom, England, Apr. 1990.

25. 전산원, 전산원 보안관리 연구(개요), NCA-RE-9025, Dec. 1990.

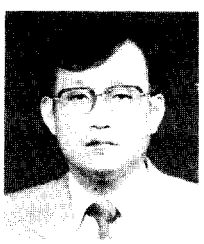
26. 전산원, 패스워드 사용지침(안), NCA-RE-9028, Dec. 1990.

27. 전산원, 컴퓨터 보안관리지침 연구 : 물리적 보안 분야, NCA-RE-9022, Dec. 1990.

## □ 著者紹介

**李 弼 中(正會員)**

1951年 12月 30日生
1974年 2月 서울大學校 電子工學科 學士
1977年 2月 서울大學校 電子工學科 碩士
1982年 6月 U.C.L.A. System Science, Engineer
1985年 6月 U.C.L.A. Electrical Engineering, Ph.D.
1980年 6月～1985年 8月 : Jet Propulsion Laboratory, Senior Engineer
1985年 8月～1990年 2月 : Bell Communications Research, M.T.S.
1990年 2月～現在 : 浦項工科大學 電子電氣工學科, 副教授

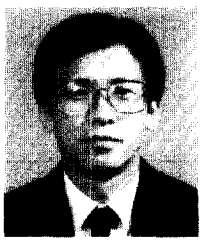


**정 진 욱(正會員)**

成均館大學校 電氣工學科 卒業(學士)
成均館大學校 大學院 電子工學科(碩士)
서울大學校 大學院 計算統計學科(博士)
韓國科學技術研究所 研究員/韓國科學技術院 시스템공학센터 데이타통신研究室長
Racal Milgo Co. 研究員(미국 Florida 所在)
現在 成均館大學校 情報工學科 副教授

**박 명 순(정회원)**

1965年 서울大學校 電子工學科 卒業
1982年 Utah大學校 電氣工學科에서 碩士學位 取得
1985年 Iowa大學校 電氣 및 컴퓨터工學科에서 博士學位 取得
1985年～1987年 Marquette大學校 電氣 및 電算學科에서 助教授로 勤務
1987年～1988年 浦項工大 電子電氣 및 電子計算學科에서 助教授로 勤務
1988年～現在 高麗大學校 電算科學科에서 助教授, 副教授로 在職中
관심분야 : 컴퓨터 구조, 운영체제 등




**이 재 용(정회원)**

1977年 2月 延世大 電子科 卒業(學士)
1984年 5月 Iowa State University, 電算機工學科(碩士)
1987年 5月 Iowa State University, 電算機工學科
1987～1982年 國防科學研究所 研究員
1983～1986年 Iowa State University, 研究助教
1987年 1月～1987年 6月 Iowa State University, 助教授
1987年 7月～現在 浦項工科大學 電子計算學科 助教授