暗號 · 情報시큐리티의 동향

인터넷으로 대표되는 네트워크와 휴대전화의 결합으로 문자 그대로 지구규모의 디지털사회가 출연하게 되었고 사회제도와 공공의 정보기반도 그것을 반영한 형태로 변화하고 있다. 차후 디지털사회를 얼마나 안전한 것으로 만들어 가는가는 국가·사회의 기반으로서 그 존속에 관계되는 중대한 문제이며, 기업 비즈니스에서는 사활(死活)을 건 비즈니스 문제가 되었다. 이들을 지탱하는 정보기반의 핵이 바로 암호를 중심으로 하는 정보시큐리티이다.
여기서는 현대 사회에서는 왜 암호·정보시큐리티가 필요한가, 그 역할과 의미는 무엇인가, 어떠한 응용분야, 과제가 있는가를 전망해본다. 또한 암호란 무엇인가, 그 안전성의 의미란 무엇인가, 컴퓨터나 통신의 디지털기술과는 어떤 관련이 있는가를 역사적 배경과 최근의 동향을 바탕으로 언급하고, 현대암호의 성립, 정보시큐리티의 적용형태, 미쓰비시(三菱)電機의 기술적 활동에 대하여 언급한다.
앞으로 전개되는 디지털 사회의 동향으로는 두 가지의 특징을 들 수 있다. 우선 휴대전화의 세계적 보급, 인터넷접속기능 장비의 발달로 현재 인터넷 유저(사용자)의 규모를 훨씬 능가하는 음성교신이 가능한 모바일인터넷의 출현이 예상된다. 모바일인터넷이 잠재적으로 갖는 안전상의 취약성을 극복하기 위해서는 암호·정보시큐리티 기술은 보다 고도의 것이 요구된다.
또한 장래의 양자(量子)컴퓨터의 출현 등 분자레벨로 육박해 오고 있는 반도체·광소자·통신기술에 앞서 현재의 디지털암호에 의한 시큐리티기반의 안전성에 대한 한계가 거론되고 있다. 디지털사회의 안전성을 확보하기 위해서는 장래를 내다본 기술의 추구가 요청되고 있으며 그 대표적인 것으로 양자역학의 원리, 광기술, 디지털기술을 통합한 양자암호가 있다. 미쓰비시電機는 2000년 9월에 일본 최초로 양자암호의 실증실험에 성공하여 조기 실현화를 지향하고 있다.

1. 안전한 디지털사회

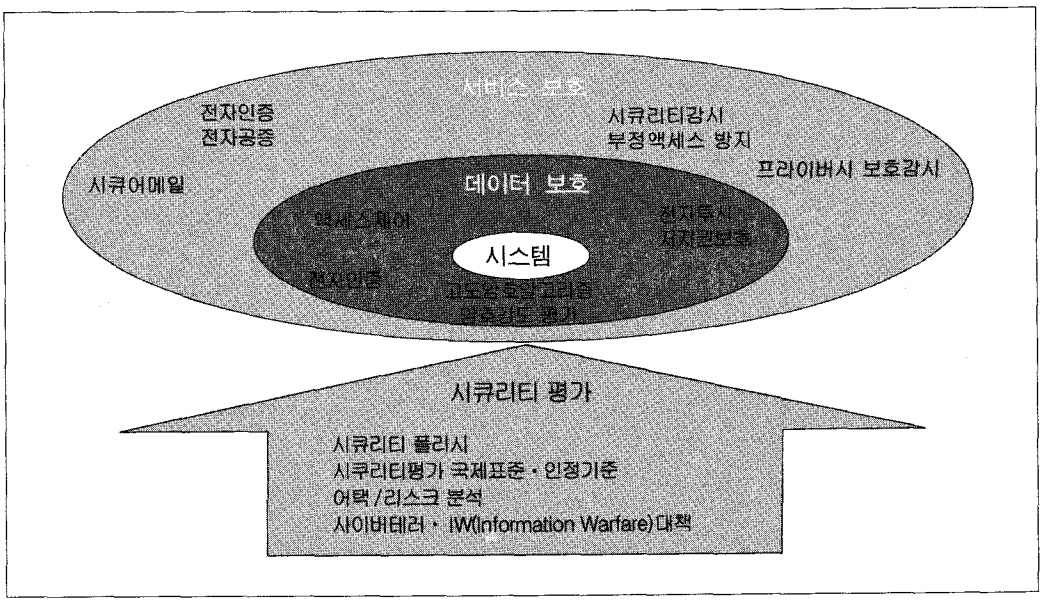
과거의 일본사회, 특히 국내에서는 "물과 안전은 공짜"라는 인식이 있었던 것으로 생각되는데, 이제 디지털화된 국경 없는 정보화사회에서 안전성을 확보하기 위해서는 코스트가 필요하다는 점을 새롭게 인식하는 것이 극히 중요한 일이 되었다.

여기에는 시큐리티와 프라이버시가 확보되어야만이 비로서 본격적인 정보화추진이 이루어질 것이다. 최고품질의 암호·정보시큐리티를 여하히 널리 많은 사람이 향수(享受)할 수 있을 것인가가 이제부터의 디지털사회에 있어서의 안전성에 대한 중요한 열쇠가 될 것이다.

가. 왜 암호인가?

소위 고전(古典)·근대암호의 시대에서 벗어나 현대의 암호·정보시큐리티의 형태가 처음으로 표면에 나타난 것은 1970년대로 알려져 있다. 동시에 다음의 3가지 패러다임의 변화가 일어났다고 한다.

(1) 종래, 군사외교의 특정조직내에 한정하여 비밀리에 사용되고 있던 암호가 인터넷으로 대표되는 디지털네트워크사회의 신뢰관계를 구축하기 위한 공통기반기술이 되었다. 동시에 학문상 및 상용의 공개마당에 있어서도



〈디지털사회를 위한 암호 · 정보시큐리티 기술〉
암호 · 정보시큐리티 기술을 유저의 관점에서 보면, 데이터를 보호하기 위한 것, 서비스 기능을 보호하기 위한 것, 이들 보호기능 · 구조를 평가하고 보증하기 위한 것으로 대별된다.

연구개발이 이루어져 사용평가되는 기술이 되었다.

(2) 기능면에서 보면 정보은닉을 주목적으로 하고 있었던 암호기능에 사람 · 물건 · 정보의 진정성(眞正性)을 보증하여 신용을 부여하는 기능이 추가되었다. 바꾸어 말하면 정보재의 유통 촉진을 위한 인증기능, 즉 서명(署名) · 개찬(改竄) 방지기능을 갖게 되었다.

(3) 디지털컴퓨터에 근거할 것을 전제로 하게 되었다. 즉 컴퓨터에 의한 암호화 비닉(秘匿) · 복호(復號), 서명 · 검증을 고속 실현한다. 부정한 해독 · 개찬에 대한 안전성평가를 위해 컴퓨터에 의한 계산량을 척도(尺度)로 한다. 해독에 요하는 컴퓨터의 계산량이 해독곤란한 방대한 것이 되도록 암호장치를 설계한다.

암호의 역할

암호 · 정보시큐리티의 현대적 사명은 아래와 같이 요약된다.

① 정보화사회에서 개인의 권리를 지키고, 법인의 권리를 지켜 국가 · 사회를 안전하게 한다.
② 신뢰관계를 구축하는 공개적 공통기반의 핵이 된다.
③ 사람 · 물건 · 정보의 진정성 보장, 신용 부여, 정보재 유통촉진의 인증을 부여한다.
④ IT(Information Technology)기술에 의한 실용화, 구현화가 이루어진다. 즉 센서 · 제어 · 영상+ 통신 · 컴퓨터+ 반도체칩의 기술에 융합된 안전유지기능으로서 실장된다.

나. 마켓동향

응용분야

우리들은 이제 컴퓨터가 모든 곳에 사용되는 시대로 들어서고 있다. 컴퓨터는 보다 싼값으로 소형화되어 전자레인지와 같은 가전에서부터 전자유도미사일과 같은 병

기에 이르기까지 모든 전자기기에 장착되어 네트워크에 의한 접속기능이 주어지고 있다. 컴퓨터는 IT화라는 깃발 아래 다음과 같은 마켓분야를 포함하는 모든 업무프로세스에 포함되는 경향으로, 그 결과 종래에는 오피스내의 회화나 서류속에 머물러 있던 비밀을 요하던 정보가 이제는 컴퓨터에 탑재되어 공중의 네트워크상을 흘러 원방의 제3자에 의한 도난, 개찬, 남용의 대상이 되면서 위험성을 증대시키고 있다. 이것을 방지 · 경감하기 위해서는 시큐리티 및 프라이버시 보호기능이 요구된다.

시큐리티대상이 되는(Potential) 마켓분야

① 교통 · 운수분야 : ITS(Intelligent Transportation System)/ETC(Electronic Toll Collection System)

② 고도가정통신시스템 : Home네트워크 통합(위성, 지상파, 케이블, 인터넷, 전화망)

③ 에너지분야 : 전력자유화 · 성력화(省力化), 전력 CALS 등에 의한 IT화 추진

④ 휴대전화 · 단말의 보급과 모바일인터넷

⑤ 마이크로프로세서로 대표되는 컴퓨터 : 네트워크화, 소형염가, 멀티미디어기능 짜넣기, 커모더티화(상품화)

⑤ 사회적으로 중요(Critical)한 시스템 : 행정부, 방위, 금융, 헬스케어의료에서의 정보네트워크화, 정보공개(인터넷)의 추진

다. 과 제

사실상 모든 기기나 IT화된 업무프로세스가 지구규모의 네트워크에 접속되는 날이 그리 머지 않은 시기에 도래할 가능성이 높다고 보며, 이것이 의미하는 바는 극히 의미심장하다고 생각된다. 예를 들면 지구의 반대측에 있는 전자적침입자가 어떤 비행장의 시큐리티시스템을 무효하게 만든다든지 군사방위시설의 게이트를 개정(開錠)하는 일이 가능해진다든지 고속도로를 시속 100km 이상으로 주행하는 차의 엔진을 정지시켜 다수의 차량이 충돌사고를 일으켜 교통을 마비시키는 일들이 예측된다. 사회 · 공공인프라의 변혁에 수반하여 시스템 IT기반의 안전성 · 신뢰성이 요구되는 것은 필수적이다.

사회 · 공공시스템 IT기반의 안전성, 신뢰성을 지탱하는 요건을 다음에 든다.

① 고도시큐리티(일본의 국가 · 사회로서의 안전에 대한 프레임워크)

② 센서 · 제어 · 영상 · 통신 · IT에 융합한 시큐리티

③ 인터오퍼러빌리티

④ 국제적 시큐리티평가기준의 형성과 대응(ISO/IEC JTC1 IS15408, IS17799 기타)

2. 暗號와 情報 시큐리티

가. 암호란

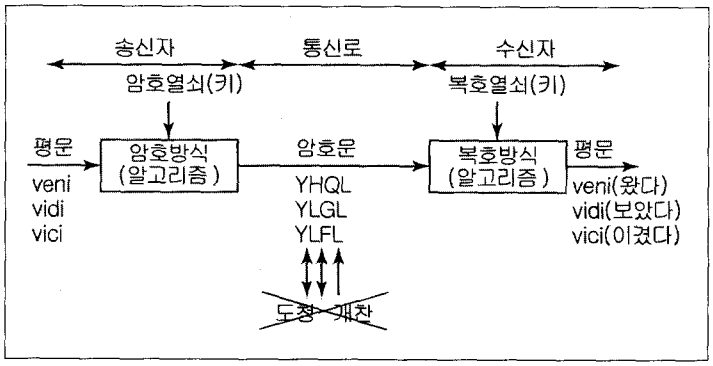
전쟁에서 암호가 쓰여진 최초 기록은 기원전 1세기 줄리어스 시저(Julius Caesar)의 갈리아 전기(戰記)이다. 시저가 적에게 포위되어 항복의 갈림길에 있던 키케로에게 메시지를 보낸 일이 기술되어 있다. 시저암호가 어떤 것이었는지는 기원후 2세기에 스에토니우스가 쓴 시저의 전기에 기록되어 있는데, 황제 시저는 다음의 예에서 보는 것과 같이 글을 쓸 때 단어를 이루는 알파벳의 순서에서 3문자씩 뒤의 것으로 썼다고 한다.

시저암호예 :

- 평문 veni(왔다) vidi(보았다) vici(이겼다)
- 암호문 YHQL YLGL YLFL
- 평문 알파벳

  abcdefghijklmnopqrstuvwxyz
- 암호알파벳

  DEFGHIJKLMNOPQRSTUVWXYZABC



〈그림 1〉 암호

암호에서는 원문을 평문(平文), 암호화된 문장을 암호문, 또 통상의 알파벳을 평문 알파벳, 문자의 위치가 바뀐 알파벳(위에서는 3문자를 시프트)을 암호알파벳이라고 한다. 현대 용어로는 여기서 문자를 시프트 내지는 문자를 바꾸어 놓는다고 하는 수속을 알고리즘 시프트문자수(여기서는 3) 또는 바꾸기패턴(여기서는 평문알파벳과 암호알파벳의 쌍)을 열쇠(키)라 한다.

그림 1에서 송신자는 평문 "veni(왔다), vidi(보았다), vici(이겼다)"를 3문자 시프트시켜 암호문 "YHQL, YLGL, YLFL"로 변환하여 보냄으로써 도청을 방지하고, 한편 수신자는 이것을 3문자 되돌려 복호하여 송신된 원래의 평문을 알 수 있다.

이들 평문(平文), 암호문, 알고리즘, 그리고 열쇠라는 암호의 기본개념은 기원전에 사용된 시저암호에서도 현대의 디지털암호에서도 공통이며, 암호의 안전성은 이중에서 특히 열쇠를 송신자와 수신자 이외에는 비밀로 함으로써 유지된다. 즉 암호를 푼다, 해독한다라는 행위는 현대에서는 알고리즘의 공개라는 전제하에 평문 및 암호문의 데이터를 입수한 제3자(송신자, 수신자 이외의 자)가 비밀의 열쇠를 푼다는 것을 의미한다. 역으로 이 제3자가 열쇠를 푸는데 따르는 어려움 즉 해독에 필요로 하는 시간 내지 해설에 요한 암호문 및 평문의 데이터량의 다과(多寡)가 암호의 안전성을 측정하는 척도가 된다. 좋은 암호란 안전성이 높으면서도 열쇠를 보유하는 송신자측의 암호화 및 수신자측의 복호화가 효율적으로 시행되는 것이 조건이 된다. 열쇠를 갖지 않은 적이 암호화된 메시지를 해독할 수 없는 또는 해독하는데 방대한 일수(日數)를 요함이 필요한 한편 시저와 기케로가 암호화·복호화에 시간이 걸려서는 안되는, 순시로 할 수 있지 않으면 안되는 것이다.

나. 암호해독과 컴퓨터 · 통신

제2차대전중 독일군이 사용한 통신암호기는 Enigma라는 이름이었다. 이에 대한 영미(英美)공동의 무선모니터에 의한 정보수집에 기초한 에니그마해독작전은 Ultra라는 코드명으로 불리고 있었다. Ultra는 연합국의 대독(對獨)승리에 크게 공헌하였다. Ultra의 성공으로 대서양에서 U보트(독일해군잠수함)에 의한 공격침몰을 면한 연합국측 선박은 300척에 이른다고 한다. 영미에 의한 에니그마암호 해독사실은 대전중뿐만 아니라 전후에도 오랫동안 비밀이 유지되어 왔으며 '70년대에 들어서 비로서 공개되었다.

울트라활동의 중핵은 제2차대전중에 런던의 북쪽 80km 브렛체리파크에 설치된 정부암호학교라는 시설에 있었다. 브렛체리파크에서 에니그마암호해독의 돌파구를 연 것은 아랑 튜링이었다. 튜링은 브렛체리파크에 오기전 1936년에 "계산가능수에 대하여"라는 논문을 발표하여 오늘의 디지털컴퓨터의 이론모델을 만들어 내고 있었다. 튜링과 그가 이끄는 해독팀은 에니그마암호기의 메커니즘을 해명하여 최초의 원시적 컴퓨터라고 할 에니그마해독장치를 만들어냈다. 이것이 가동하기 시작한 1940년 4월 이후 영미는 독일의 암호통신 해독이 가능하게 되어 울트라작전이 개시되었다. 최초의 컴퓨터가 암호해독기였다

는 사실은 양자의 불가분한 관계를 나타내는 것이다.

계산에 관한 튜링이론은 현대의 암호해독의 기반이 되었는데 현대디지털 암호의 최초가 된 DES 암호 Data Encryption Standard의 기본적 아이디어는 통신에 관한 정보이론의 창시자 샤논 이론에 근거한다.

샤논은 1949년 "비닉(秘匿)시스템의 통신이론"에서 '70년대에 DES 암호로 출현하는 것의 안전성근거(엔트로피라는 불확실성에 대한 확률분포의 수학적함수의 개념으로 주어지는 것)와 알고리즘구성법에 관한 아이디어를 기술하고 있다. 이 논문자체도 방위군사에 관계된다 하여 당초 얼마동안은 한정된 범위에서만 알려져 있었다.

다. 현대암호

(1) DES

'73년 5월 15일, 미국의 국가표준규격국 The National Bureau of Standard(현재는 상무성에 속한 NIST : National Institute of Standards and Technology)는 연방정부조달시스템용 암호를 공모하였다. 이것이 오늘날까지 가장 많이 사용되어 왔다는 DES 암호의 개발로 이어졌으며 최초의 현대암호로 정의되었다.

현대암호와 고전암호와의 차이를 비교하면 다음과 같다.

고전암호의 세계는

- ○ 암호의 역사는 인류의 역사와 같은 길이
- ○ 군사외교목적의 비공개기술
- ○ 참가자 한정의 1대1 통신을 전제
- ○ 문자의 치환을 중심으로 하는 변환처리

이고, 현대암호의 세계는

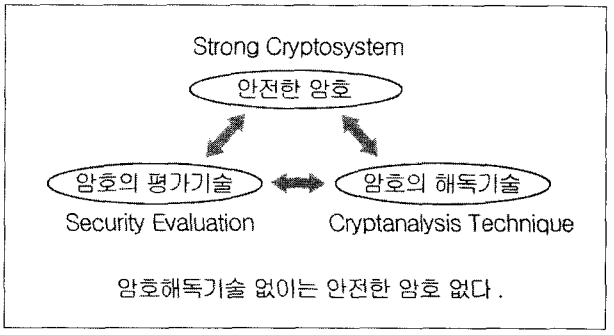
- ○ 본격적인 연구는 '70년대부터 시작
- ○ 프라이버시 보호목적에 이용
- ○ 불특정다수가 참가하는 네트워크형 지향(指向)
- ○ 디지털신호의 변환처리
- ○ 계산량이론을 사용한 안전성평가

이다.

현대암호의 효시인 DES는 IBM에 의해 개발되었다. 개발 당시에는 LUCIFER라는 이름이었는데 미국의 국가안전보장국 National Security Agency가 평가에 개입하여 변경이 가해진 것이라 한다. DES는 우선 '75년 3월 17일에 미국연방정부 등록암호로서 발표되어 그후 '77년 1월 15일에 연방정부의 unclassified(외교방위군사 등의 비닉용은 아니다) 시스템용의 표준으로 채택되었다. 그후 5년마다 연방정부표준으로 재검토되어 약 20년간 사실상의 국제표준의 위치에 있었으나 암호해독법의 진보로 안전성강도가 저하되어 '99년 10월 25일에 Triple-DES(열쇠길이를 3배로 한 DES를 3중으로 건다)로 치환되었다.

(2) 현대암호의 해설

DES로 대표되는 암호에 대한 유력한 해독법은 열쇠총당법(鍵總當法), 차분해독법(差分解讀法), 선형해독법(線形解讀法)의 세 가지를 들 수 있다. 처음의 두 가지 해독법은 이미 DES 설계시에 고려되었다고 한다. 세번째의 선형해독법의 발명과 그 실증실험은 미쓰비시電機



〈그림 2〉 암호의 안전성과 암호해독

의 松井씨가 했다. 미쓰비시電機에서의 암호·정보시큐리티에 대한 활동도 여기서부터 시작되었다. 암호해독, 안전한 암호시스템의 설계와 개발, 안전성의 평가는 삼위일체의 기술로 생각되어(그림 2 참조), 우리들은 그 컨셉트 하에서 MISTY를 처음으로 하는 암호알고리즘, 그것들의 정보시큐리티시스템으로서의 실장, 암호·정보(시큐리티)시스템에 대한 해독·공격의 평가기술을 개발하고 있다.

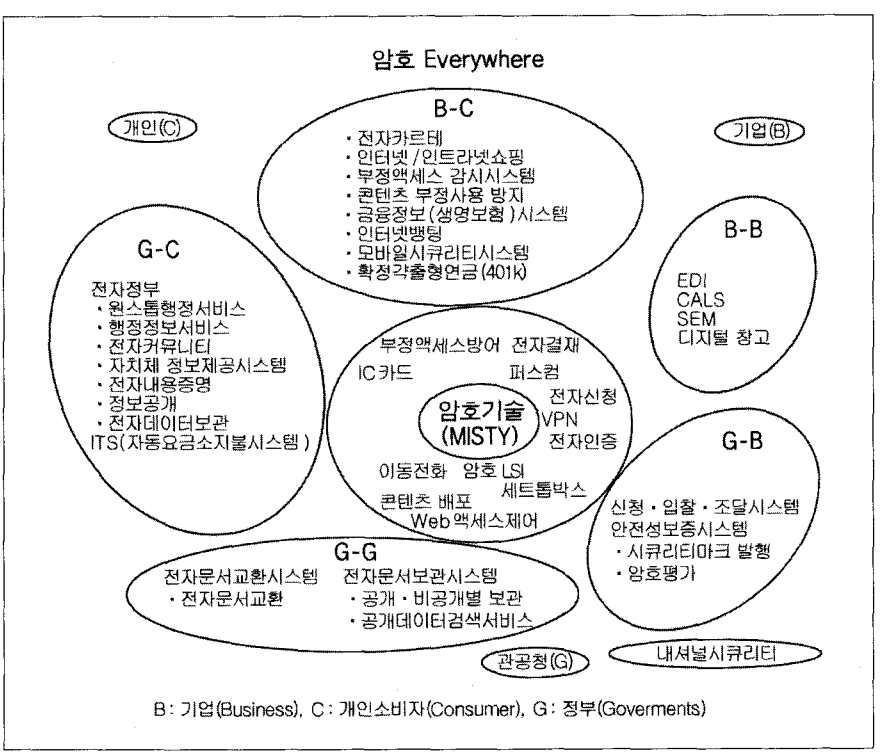
(3) 적용 : 배경과 형태(정보시큐리티의 중요성)

'91년 1월에 개시된 만안(湾岸)전쟁에서는 미군의 미국본토기지와 사우디아라비아주둔 부대와의 통신은 25%가 인터넷을 통한 것이었다. 게다가 현재는 믿기 어려운 일이지만 인터넷상에서 평문에 의한 통신을 하고 있었다고 한다. "백만불 지급하면 미국과 사우디아라비아를 잇는 미군의 병참정보네트워크를 대혼란에 빠뜨릴 수도 있다"라는 네덜란드의 해커그룹의 제안에 만약 이라크의 후세인이 응했더라면 만안(湾岸)전쟁에서의 미국의 선명한 승리는 없었을지도 모른다. 간편하고 강력한 유용성에 반비례하여 인터넷은 안전성에 관한 취약성을 안고 있었던 것이다. 만안전쟁 후 미국은 국가적인 대책에 힘쓰고 있다.

또 미국에서는 2001년도 말에 인터넷에 의한 구매자층의 1위가 여성으로 옮아갔다는 조사통계가 나왔다. 이는 본격적인 인터넷 전자상거래 시대에 접어들었다는 것을 의미하는 것으로 관측되고 있다. 일본에서도 휴대전화의 i-mode 가입자가 3000만명을 넘었다고 한다. 인터넷의 취약성을 극복하는데는 암호·정보시큐리티가 필수적이고 그것이 전자사회질서를 규정하며 미래의 사회를 좌우하는 것이 되어, 인류에게 커다란 영향을 준다는 것이 인식되기 시작하고 있다.

암호를 실제의 시스템에 적용할 때의 형태는 적용범위, 대상, 실장(實裝), 시스템의 로지스틱스에 따라 다음과 같이 여러 갈래로 되어 있다(그림 3 참조).

- ○ 암호LSI로직 : 반도체칩 실장, 설계정보 IP(Intellectual Property)
- ○ 암호짜넣기 기기 : 휴대전화, 통신기기, 내(耐)탬퍼 암호보드, IC카드
- ○ 암호를 관리운용하는 시스템 : 인증시스템, 열쇠관



〈그림 3〉 암호·정보시큐리티 적용대상분야

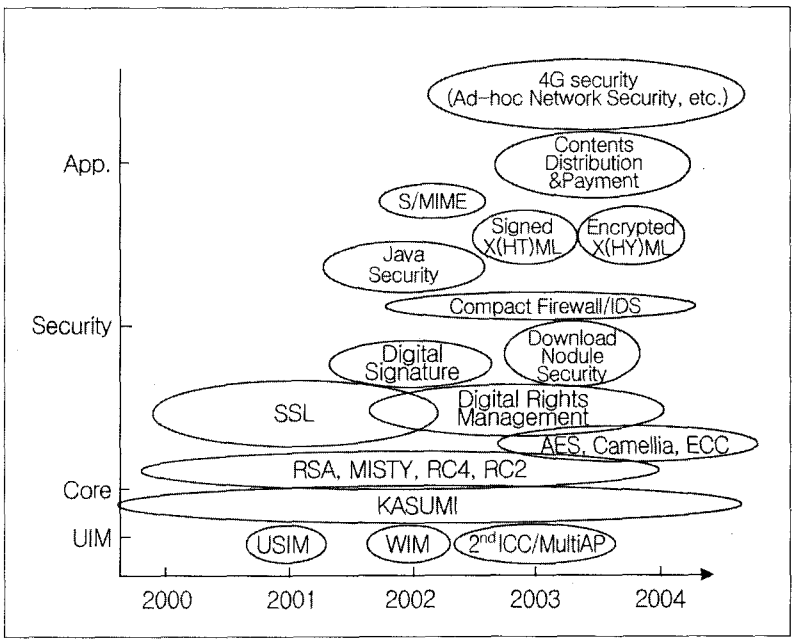
리시스템, 부정액세스의 평가 · 방어시스템

○ 상기 서비스 : 시큐리티설계, 시큐리티 관리 · 운용 폴리시의 책정 · 컨설팅

3. 앞으로의 동향

가. 인터넷이 모바일이 된다

세계의 휴대전화 이용자수가 2002년에 들어서면 10억을 돌파할 것이라는 전망이 보도되었다(2001년 12월 29일, 日經新聞). 휴대전화시장조사회사인 영국EMC에 의하면 2001년말 예상은 9억 8856만명, 세계인구 약 6명 중 1명이 휴대전화를 이용한다는 계산이 된다. 인터넷접속기능을 높인 휴대전화가 주류가 될 것이다.



〈그림 4〉 Mobile Security Roadmap

인터넷 e-Commerce 초기에 비하여 모바일인터넷에서의 시큐리티, 프라이버시의 필요성에 대한 관심은 더욱 높아졌다고 한다. 인터넷의 모바일판은 오늘의 인터넷의 도달범위를 훨씬 능가할 것으로 예상된다. 그 근거로는 조작이 복잡하고 비싼 퍼스컴을 필요로 하지 않는다는 것, 인터넷의 편리성을 보다 광범위한 사용자에게 가져다 준다는 것을 들고 있다. 전신(Telegraph) 마켓을 이어받은 것이 전화(Telephone)였던 것과 같이 반복해서 현대판 Telegraph인 인터넷을 이어받는 것이 또 Telephone이 되지 않겠는가라고 예측하고 있다. 이 예상이 맞다면 무선을 이용하는 점(Wirelese)과 사용자규모의 현격한 크기가 더하여져 인터넷에서의 안전상의 취약은 몇십배나 증폭되어 인계될 것이다. 오퍼레이터, 휴대전화메이커, 서비스프로바이더 연대하에 시큐리티 및 프라이버시 보호대책이 강구되어 나가야 하는 것이 필수적일 것이다.

모바일인터넷에 관한 암호 · 정보시큐리티기술의 예측 로드맵을 그림 4에 표시하였다. 데이터통신기능을 포함한 휴대전화상의 암호 · 시큐리티기능의 실현과 휴대전화상에 그것들을 실장해가기 위한 암호 하드웨어칩을 포함한 콤팩트화의 기술이 요구된다.

나. 보다 높은 안전성을 추구하여

암호해독용 열쇠를 컴퓨터로 순차적으로 조사해 가면 어떠한 암호라도 언젠가는 해독의 단서가 열릴 것이다. 그러나 그것은 수천년 · 수만년의 세월을 필요로 하기 때문에 현대의 디지털암호의 안전성은 유지되고 있다고 할 수 있다. 그러나 광자(光子) 등의 양자를 이용한 컴퓨터가 실현되면 암호해독용 열쇠를 알아내는 것은 순시에 가능해진다고 한다.

'70년 이래 DES암호나 전자서명용의 RSA암호 등으로 대표되는 것과 같이 암호개발은 기술적으로 암호해독에 앞서 왔다. 이로서 오늘날 인터넷 등의 네트워크상에서의 안전한 통신·거래가 이루어질 수 있게 되었으며 이 기반 위에 앞으로 디지털사회가 구축되려고 하고 있다. 장래의 양자컴퓨터의 출현은 이것을 밑바탕부터 파괴할 것으로 생각된다.

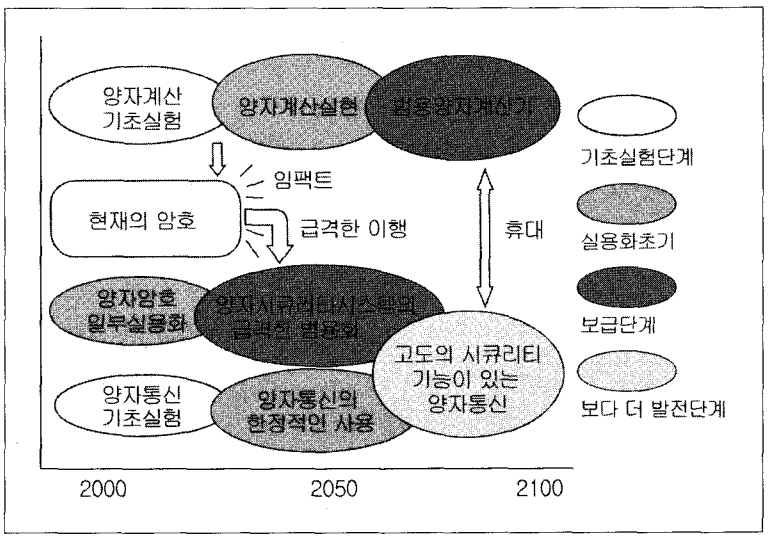
그 동안 양자컴퓨터의 출현은 오늘 내일과 같은 가까운 장래는 아니라고 예측되어 왔다. 그럼에도 불구하고 양자컴퓨터에 의한 계산을 하면 현재 전자서명이라는 중요한 기능을 실현하는 공개열쇠 암호가 순시간에 해독된다고 하는 증명이 이루어져 암호·정보시큐리티의 세계 및 군사방위분야에 큰 충격을 주었다. RSA암호 해독을 위한 소인수(素因數) 분해계산을 하는데 129 단위수의 소인수 분해에 600대의 디지털컴퓨터로 수개월 걸리는 것이 '94년의 AT&T벨연구소 피터쇼어발표의 양자컴퓨터프로그램으로 하면 그 수의 수백만배 크기의 수를 그 수의 소인수분해하는데 걸린 시간의 백만분의 1로 풀 수가 있다는 것이다. 발표당시에는 양자컴퓨터가 존재하지 않아 쇼어자신에 의한 실증실험은 이루어지지는 못하였으나 과학잡지 "Nature" 2001년 12월 발행된 기사에서는 「IBM의 과학자와 스탠포드대학원생 팀에 의한 "쇼어의 알고리즘"의 첫 데몬스트레이션」이 시행되어 그 원리의 실증실험에 의한 증명이 성공했음을 보도하고 있어 양자컴퓨터의 실현이 꿈같은 이야기만이 아님을 말하고 있다.

이와 같은 해독기술에 대항하기 위해서는 양자암호의 개발이 필요하다. 양자역학이 지배하는 미소한 세계에서는 입자의 상태에 영향을 주지 않고 그 입자를 관찰하여 상태를 결정하는 것은 불가능하다고 한다("불확정성원리"). 이 원리를 이용한 것이 양자암호이다. 통신의 송수신 사이에 완전한 비밀리에 의사전달이 가능하게 될 수 있는 방법으로 개발을 서두르고 있다.

양자암호는 광과 디지털기술의 융합으로 실현가능하며 수년 이내에 실용화될 것으로 생각되고 있다.

미쓰비시電機는 '99년 양자암호연구에 착수, 일본에서는 처음으로 광자에 의한 양자암호통신의 실증실험에 성공하였는데, 2000년 9월 시점에서 세계 최고수준의 통신성능을 시판중인 광파이버를 사용하여 실현하였다.

양자암호관련전망을 그림 5에 표시하였다. ■



〈그림 5〉 양자정보통신·처리의 장래 전망