暗號 · 시큐리티技術의 현황과 전망

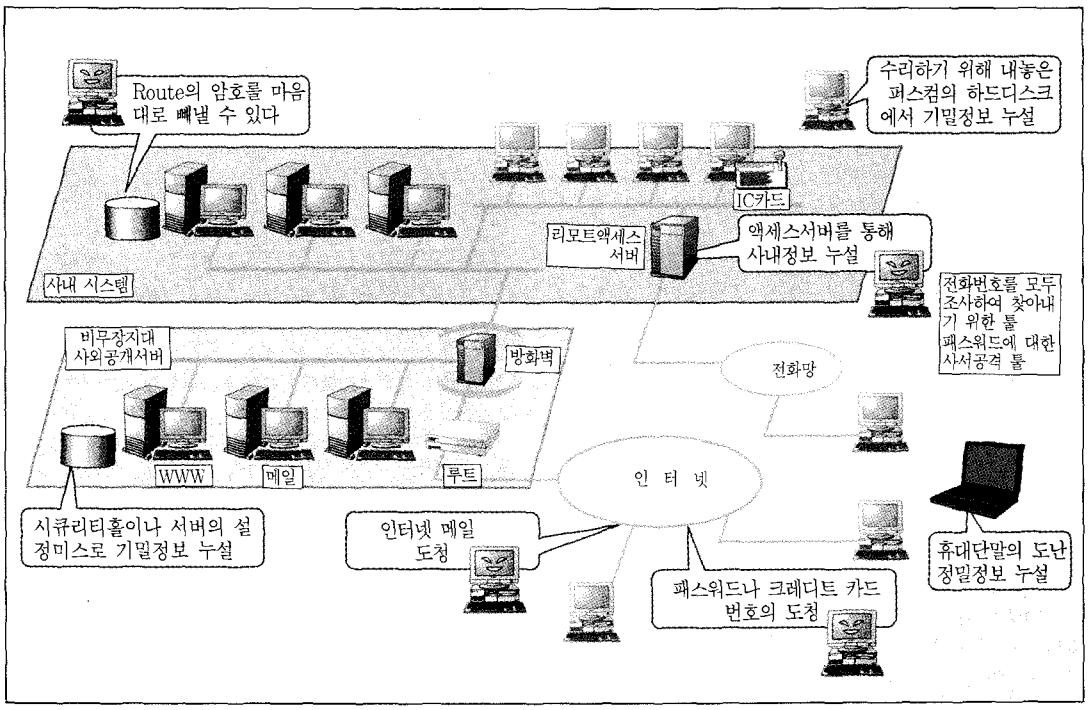
인터넷을 비롯하여 컴퓨터 네트워크와 통신의 급격한 발전으로 정보시큐리티의 중요성이 주목받고 있다. 정보시큐리티 대책의 기본은 기술적 대책에서부터 시작된다. 암호기술은 비밀 유지와 인증이라는 기본기능을 갖고 있으며, 직접적으로 정보를 지키는 일과 함께 다른 정보시큐리티기술의 요소로도 사용된다. 암호와 함께 사용되는 시큐리티기술로서 인간의 신체적 특징을 활용한 개인식별, 공공 공간과 중요시설 등의 대규모 범위에 대한 원격감시 그리고 이것들을 통합하는 응용시스템이 있다.

본고에서는 이들 기술의 현황과 동향을 중심으로 정보시큐리티의 대책에 대하여 기술한다.

1. 머리말

현재 일본 국내에서 컴퓨터 및 네트워크를 이용한 범죄는 일반적으로 알려진 바에 따르면 '95년 32건, '96년 89건, '97년 101건으로 해마다 증가하고 있다. 아직은 유럽, 미국과 비교하여 많다고는 할 수 없는 단계이지만, 범죄에까지는 이르지 않은 不正액세스부분은 극히 심각한 상황이다. 네트워크상에서의 국경의 의미는 이미 상실되었으며 국외로부터의 액세스를 지리적으로 차단하는 방법도 없다. '97년 미국 국무부에의 해커침입은 연간 16만건 이상으로 추정되고 있다. 일본 시장에서 일어나는 카드범죄는 이미 연간 약 200억엔의 손해가 보도되고 있고, 카드는 머지 않아 네트워크와 사람과의 인터페이스 역할만을 하게 될 것으로 보여 그 급증은 가히 위협적이라 하겠다. 그러므로 전자결재나 전자상거래도 포함한 앞으로 정보화 네트워크사회의 진전에 맞추어 보다 완전한 정보시큐리티 대책과 그 인프라의 정비는 꼭 필요하게 되었다.

정보시큐리티기술은 표 1과 같은 종합적 대책이 필수적이다. 공격자는 시스템의 가장 취약한 곳을 찾아 공격한다고 한다. 특히 시스템에서 문제가 되는 것은 인간에 대한 대책일 것이다. 정보시큐리티도 기술적 대책에 인사·운영을 포함한 명확한 시큐리티정책과 관리의 유지가 정보를 지키는 요체가 된다. 즉 조직으로서 무엇을 얼마 만큼의 코스트를 들여 지킬 것인가를 명확히 해야 한다. 이 정책에 기초하여 관리·운영규정 등을 결정해 간다. 법과 제도의 정비, 네트워크사회에서의 윤리 확립을 위한 교육, 계몽, 나아가 유럽, 미국 등에 비하여 결정적으로 부족하다고 지적되고 있는 시큐리티 관리자의 양성도 요구된다.



〈예상되는 위협〉

정보시큐리티 대책을 강구하기 위해서는 우선 위협 리스크의 분석이 요구된다. 개인의 시스템이 놓여진 환경, 주변조건, 운용에 따라 어떤 위협이 지배적인가가 다르다.

이들 대책의 전제로서도 기술적인 대책이 우선적으로 요구된다.

2. 情報시큐리티

2.1 情報시큐리티란

정보시큐리티란 정당한 정보시스템 유저에게 "안전과 신뢰"를 줌과 동시에 여러 가지 위협에서 정보를 지키는 것이다. 天災 · 사고 · 고장 · 오류 등의 비인위적 및 과실적 위협과 도청, 문구를 고치는 것, 위조, 부정행위 등의 인위적이고도 의도적인 두 가지 위협이 있다. 현재 큰 문제가 되고 있는 것은 후자이므로, 이에 대한 정보시큐리티에 초점을 맞추어 기술하고자 한다.

〈표 1〉 정보시큐리티 대책

시큐리티 정책					
시설 · 설비 장치 소프트웨어 네트워크	감시 · 감사	관리 · 운용 보험	인사 조직	법 · 제도 윤리	교육 · 계몽
정보시큐리티 기술					

2.2 국제적 · 정치적 확산

범죄수사 등을 위해 합법적으로 법집행기관에 액세스 권한을 주는 것을 합법적 엑세스라 한다. 예를 들면 공적인 대규모시스템에서의 엑세스권한의 부여인데 '94년 미국연방정부에 의해 제안된 통칭 '클리퍼 칩' 방식이라고 하는 키供託시스템(Key Escrow System : KES)이 세계적으로 커다란 논의를 불러일으킨 적이 있었다.

비즈니스界와 학회의 자체관리에서 정부에 의한 정보의 일원적 관리로 가게 된다고 하는 염려와 두려움이 제기되고 또 기술적인 문제점도 표출되면서 미국연방정부도 추진을 단념하게 되었다. 그러나 그후 '96년에 암호키를 분실하였을 때 그것을 회복한다고 하는 형태의 키 회복시스템(Key Recovery System : KRS)을 새로이 제안하여 강력히 추진하려고 하고 있다. 이에 대한 공적 채용에 대해서는 현재도 논의가 진행되고 있다.

정보시큐리티, 특히 암호에는 정보의 기밀성 보호 실현이라는 과제에 따라 정치적인 문제가 얽히게 된다. 또한 그것이 전세계 정보네트워크로 사용범위가 널리 확장되면서 그 취급에 국제적인 관점이 요구된다. 이 때문에 OECD(경제협력개발기구) 등의 국제기관에서 정보시큐리티에 관한 검토가 진행되고 있다. 아래에 표시하는 '97년 3월 책정한 OECD 암호정책가이드라인은 정보시큐리티를 생각할 때의 기초가 될 수 있다.

2.3 OECD 暗號政策 가이드라인

다음과 같이 요약될 수 있다.

(1) 암호의 신뢰성

정보시스템의 이용자가 충분히 신뢰할 수 있는 암호방식일 것

(2) 암호방식의 자유선택

법률의 범위내에서 암호방식을 자유로이 선택할 수 있는 권리

(3) 시장주도에 의한 암호방식의 개발

각국 정부의 니즈·수요·책임에 따른 시장주도의 개발

(4) 암호방식의 표준화

암호방식의 기술적 표준·기준·프로토콜은 국가 또는 국제수준에서 개발/보급

(5) 프라이버시와 개인데이터의 보호

통신의 비밀 및 개인데이터의 보호를 포함한 프라이버시에 관한 개인의 기본적 권리 존중

(6) 합법적 액세스

각국의 암호정책에 있어서 암호화된 데이터의 平文 또는 암호키에의 합법적 액세스를 용인

(7) 책 임

암호서비스를 제공하는 또는 암호키를 보유/이용하는 개인이나 기관의 책임은 명확하게 기술

(8) 국제협력

각국 정부는 암호정책의 국제적 조화를 기하여 정당하지 않는 무역장벽을 제거

3. 情報시큐리티技術

정보에 대한 액세스권한을 어떻게 부여할 것인가가 정보시큐리티기술의 중심 과제이다. 유저(사람·조직 및 설비의 엔티티 또는 네트워크시스템의 요소 등)의 인증과 정보의 보호가 기본이 된다.

3.1 유저의 認證

유저의 인증이란 정보에 액세스하고자 하는 유저가 어떤 형태로든 신원이 보증되어 있는 존재임을 명확히 하는 것을 말한다. 상대가 사람일 경우 이것을 개인인증이라 하며 패스워드와 같은 기억, IC카드 등의 휴대, 그 사람의 지문, 망막, 虹彩패턴 등 바이오메트릭스에 의한 방법이 있다.

사람 이외의 인증도 그 대상이 갖는 고유정보 또는 고유의 능력을 이용한다. 이때 부정액세스가 일어날 수 있는 환경에서는 암호에 의한 인증이 기본이 된다. 이것은 그 대상이 소정의 비밀 암호키를 사용할 수 있는 기능을 갖고 있음을 확인함으로써 이루어진다.

3.2 情報의 보호

정보의 보호란 미리 정한 형태(예를 들면 읽어내기, 써넣기 등)의 액세스를 정해진 정보(키)를 갖고 있는 자에게만 허용하고 그 이외의 액세스(부정액세스라 함)

는 배제하는 것을 말한다. 즉, 防止와 檢知에 의한 抑制이다.

방지는 시설·설비에 관한 것에서부터 센서 및 소프트웨어에 의한 방법 등이 있으며, 그 각각이 모두 중요하나 앞으로의 오픈형 네트워크에서는 특히 암호를 사용하는 방법이 중요하게 취급될 것이다.

檢知에 의한 抑制는 부정액세스가 생겼을 때 그것을 검출하여 경보를 울리든가 그 정보를 무효로 만든다. 또한 부정액세스의 證跡을 보존하여 부정액세스한 자에게 어떤 형태의 제재를 가하는 등으로 부정액세스의 의욕을 상실케 하여 억제하는 것을 말한다. 그 방법으로는 인증기술, 부정액세스의 특징을 포착, 그것에 기초한 검지·대처, 컴퓨터바이러스 대책, 디지털 투과법(대상이 되는 정보에 부정검지 정보를 삽입시켜 부정사용시에는 미리 넣어진 검지용정보로 부정을 폭로한다. 때로는 부정사용자도 발견한다) 등이 있다.

3.3 액세스制御方式의 구성

유저의 인증과 정보의 보호를 기초로 하여 액세스 제어시스템이 구성된다. 여기서 액세스제어란 부여한 액세스권한을 실현하는 방법을 말한다. 유저의 수와 지켜야 할 정보의 수, 시스템의 일원적 관리자의 유무, 각 유저와 각 정보에 대하여 어떠한 액세스가 허용되는가, 유저나 정보의 증감에 따른 갱신정도 등 각 시스템의 패러미터와 형태에 따라 효율좋은 방식을 사용할 필요가 있다. 특히 대규모시스템에 있어서의 액세스제어의 기본적 과제이다. 예를 들면 네트워크에서는 Virtual Private Network나 미쓰비시電機의 MELWALL시리즈가 이에 해당된다.

4. 暗號技術

암호의 기능에는 守秘와 認證이 있다.

4.1 守 秘

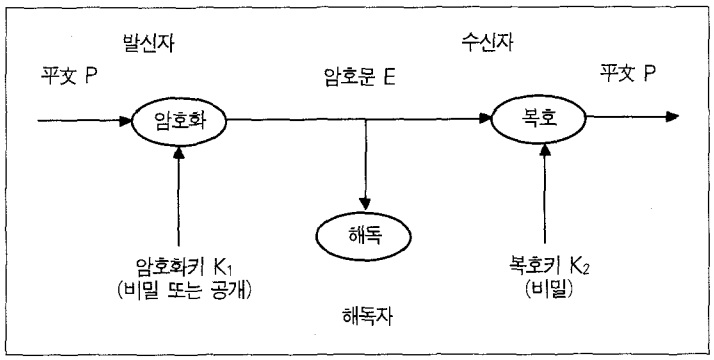
그림 1에 암호에 의한 守秘機構를 타나내었다. 발신자가 비밀로 보내고 싶은 정보 P(平文)를 암호화키 K_1을 사용하여 암호문 E로 변환하는 것을 암호화, 수신자가 復號키 K_2를 사용하여 E를 원래의 P로 되돌리는 것을 復號라 한다. 여기서 암호화/복호는 효율적으로 실행될 수 있어야 하며 복호키 없이 암호문에서 평문을 구하는 것이 곤란하도록 되어 있어야 한다. 또 복호키는 비밀로 하여 미리 인정된 당사자 이외는 입수할 수 없도록 조치해야 하며 다른 입수가능한 정보로도 추정이 불가능하도록 해야 한다.

역으로 암호문을 어떠한 다른 수단으로 입수하여 복호키 없이 평문으로 복원하는 것을 解讀이라고 한다.

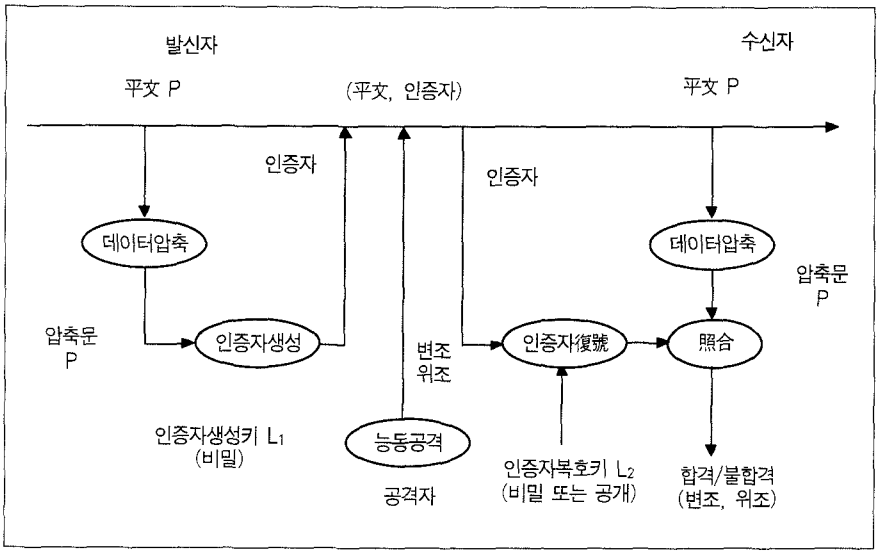
4.2 認 證

그림 2에 대표적인 인증방법(Message Authentication Code : 認證子)을 표시한다.

이것은 문서에서의 서명이나 날인 기능에 해당한다. 발신자는 전달하고자 하는 평문 P에 대하여 어떤 형태로든 데이터를 압축하여 압축문 P를 작성한다. 다음에 認證子 生成키 L_1으로 P를 인증자 a로 변환하여 이것을 평문 P에 첨부한(P, a)를 송부한다. 수신자는 수신한 평문에 대하여 마찬가지로 압축문을 구하고 동시에



〈그림 1〉 암호에 의한 守秘



〈그림 2〉 암호에 의한 인증

인증자를 인증자 생성키 L_2로 복호하여 인증자로부터도 압축문을 복원한다. 그 압축문 양자가 일치하면 수신한 평문과 인증자는 정당한 것으로 판정된다. 실행시의 효율, 키의 隱匿性(몰래 감춤)의 유지, 키 및 인증자의 유추가 어렵도록 해야 함은 어느것이나 守秘의 경우와 마찬가지이다.

4.3 공통키 방식과 공개키 방식

발신자와 수신자가 같은 키를 공유하는 암호를 공통키암호 또는 대칭키암호라 한다. 대표적인 공통키암호로는 '76년에 미국연방정부의 표준암호로 채용된 DES(Date Encryption Standard)를 들 수 있다.

DES는 표준화를 위하여 그 알고리즘이 완전히 공개되어 있다. 이것은 암호의 안전성은 키를 비밀로 유지함으로써 확고히 해야 하며 알고리즘을 공개하더라도 안전하도록 설계하여야 한다는 컨셉트에 기초하고 있다. 同社의 암호알고리즘 MISTY도 같은 설계원칙에 따르고 있다. 사실 암호알고리즘은 아무리 비밀로 해도 머지않아 알려지는 경우가 많다. 특히 네트워크상에서 많은 사람이 사용하는 소프트웨어에서 실장된 것은 숨겨두는 것이 불가능하다. 알고리즘의 공개는 암호의 보급, 연구·개발의 활성화에 크게 공헌하고 있다.

한편 발신자와 수신자의 키가 달라 한쪽에서 다른 쪽을 추정하는 것이 극히 어려운 경우 이것을 공개키암호 또는 비대칭암호라 한다. 키의 한쪽을 공개해도 다른 쪽을 비밀로 유지할 수가 있다. 공개하는 키를 공개키(Public key), 비밀로 하는 키를 비밀키(또는 개인키, Private key)라 한다. 守秘에는 암호화키 K_1이 공개키, 복호키 K_2가 비밀키이다. 인증에는 인증자 생성키 L_1이 비밀키, 인증자복호키 L_2가 공개키이다. 이와 같은 인증을 디지털서명이라 부른다. 공개키암호에서 비밀키를 갖는 것은 원칙적으로 단 한사람, 소유자 개인만이 가능하므로 키관리가 간결해짐과 동시에 발신과 수신의 시큐리티상의 구별을 명확하게 할 수 있어 통신상의 범죄·분쟁의 해결에 유용하다. 반면에 결점으로는 공통키암호에 비하여 암호화나 복호가 복잡하여 처리속도가 대단히 느려, 약 100배에서 1000배까지도 늦어진다. 따라서 데이터의 守秘에는 공통키 암호를 사

용하고 키 그자체의 配送이나 디지털서명에 공개키암호를 사용하는 것이 일반적이다. 대표적인 것에 RSA (Rivest-Shamir-Adelman)암호, 또 최근에는 RSA 암호보다 더 효율이 좋다고 하는 楕円암호가 있다.

4.4 暗號의 안전성

암호를 守秘에 사용하는 경우 가능한 한 해독이 어렵도록 설계하지 않으면 안된다. 암호의 안전성은 실용상 거의가 計算量的 안전성을 척도로 하고 있다. 계산량적으로 안전하다고 하는 것은 원리적으로는 해독이 가능하다해도 해독에 방대한 계산량을 필요로 하기 때문에 실제로는 해독이 불가능한 케이스를 말한다. 실용적인 암호에 대하여는 계산량적으로 안전하다는 것을 이론적으로 증명하기는 극히 어려워 경험이나 감 그리고 사례에 기초하여 판단되어 왔다. DES는 많은 연구자들과 여러 방향에서의 안전성 평가에 견디어 내면서 개발한지 10년 이상 가장 신뢰할 수 있는 상용암호로서의 지위를 유지하여 왔다. 그러나 해독기술의 급속한 진보로 또 컴퓨터의 고속화, 超並列計算技術 등에 의하여 DES 해독에 요하는 계산량의 벽이 해마다 낮아지고 있어 DES도 안전성에 위협을 받고 있다. 그 해독기술의 대표적인 것 중에 同社의 마쓰이씨가 발명한 線形解讀法과 그에 의한 계산기를 사용한 DES해독실험에 의한 실증이 있다. 미국에서는 이에 대응하여 Triple-DES (DES를 3회 건다)를 채용하려는 움직임이 있다. 그러나 이것이 DES보다 얼마나 안전한지에 대한 정확한 지표나 근거는 아직 없다. 또 속도가 3배 늦어진다는 트레이드 오프가 있다.

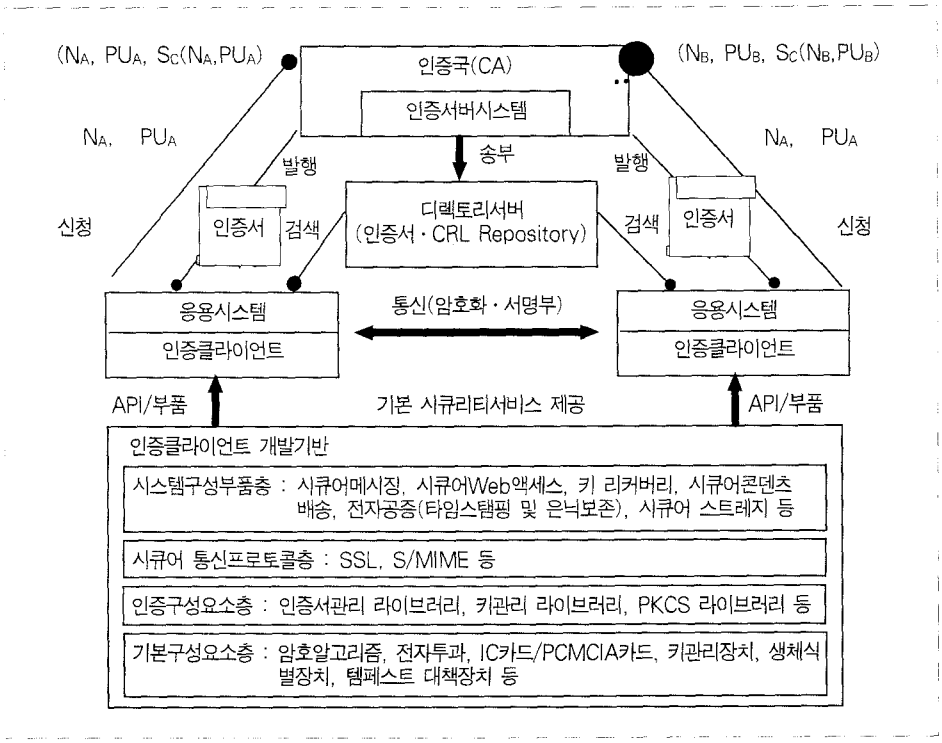
이들의 문제를 극복하는 방법의 하나로 MISTY를 평가할 수가 있다. 이제까지의 대표적인 해독법에 대하여 계산량적으로 충분히 해독이 곤란(즉 안전)하도록 설계되어 있으며 하드웨어, 소프트웨어 어느쪽에서도 고속으로, 또 규모에 있어서도 소규모 IC카드용에서 대규모 고속네트워크기기용에 이르기까지 폭넓은 플랫폼에 적용할 수 있다.

4.5 공개키 기반

암호의 守秘기능 · 인증기능을 대규모시스템상에서 사용하기 위해서는 키관리의 인프라 정비가 필요하다. 그 기초가 되는 것은 공개키방식에 의한 키관리방식이다. 인증국(Certificate Authority : CA)방식에 의한 공개키 기반(Public Key Infrastructure : PKI)이라고 한다. 그림 3에 표시하는 것과 같이 유저 A는 자기의 이름 N_A와 자기의 공개키 PU_A를 인증국에 제출하여 여기에 인증국의 서명 $Sc(N_A, PU_A)$를 받는다. 즉 유저 A의 공개키 인증서로서 이름과 공개키와 서명의 조합 $(N_A, PU_A, Sc(N_A, PU_A))$을 발행받는다. 다시 말하면 인증국이라는 권위자가 각 유저에게 인증국의 보증서명이 있는 공개키 보증서를 각 유저에게 제공하는 것이다. 이 과정을 거친 유저 A와 유저 B는 서로 각각의 공개키 인증서를 교환하여 보증된 서로의 공개키를 입수하고 그것을 사용하여 공통키암호를 위한 키를 보내거나 인증하는 방법으로 A와 B 사이의 통신의 守秘 · 인증을 실현할 수가 있다. 앞으로는 각 기업집합체마다 또는 업종마다 복수의 PKI 인프라가 併存하는 형태가 될 것으로 보이므로 그 인프라간의 정보授受를 어떻게 원활하게 하는가가 앞으로의 큰 과제가 될 것이다.

5. 個人識別과 監視/액세스管理技術

어떤 사람들이 어떻게 액세스하여 운용하는지를 아는 것은 정보시스템과 중요시설의 시큐리티를 결정하는 중요한 요소이다. 액세스하는 사람을 인식 · 판정하는 개인식별, 개개인의 신체적 특징에 기초한 식별기술은 액세스 권한을 결정하는 척도와 관련지어 사용된다. 지문에 의한 조회는 그중에서도 대표적인 것이다. 컴퓨터실 등에의 입퇴실, 금융단말이나 퍼스컴을 비롯하여 각종



〈그림 3〉 공개키 기반(인증국 방식)

정보단말에의 액세스에 대한 개인확인에 적용된다. 지문화상을 얻는 센서기술, 고속으로 정확하게 화상 조회하는 패턴조회 알고리즘, 이것들을 저가격, 고속으로 실행하는 장치와 화상데이터를 축적 · 검색하는 데이터베이스 기술로 구성된다.

同社는 염가로 고정도의 지문조회장치를 제공하고 있다. 지문에 더하여 실제의 서명조작으로 조회하는 온라인 필자조회도 제공하고 있다. 펜입력 컴퓨터나 휴대정보단말의 Doublet 위에 필기한 필적 · 필순 · 필속으로 개인을 조회한다.

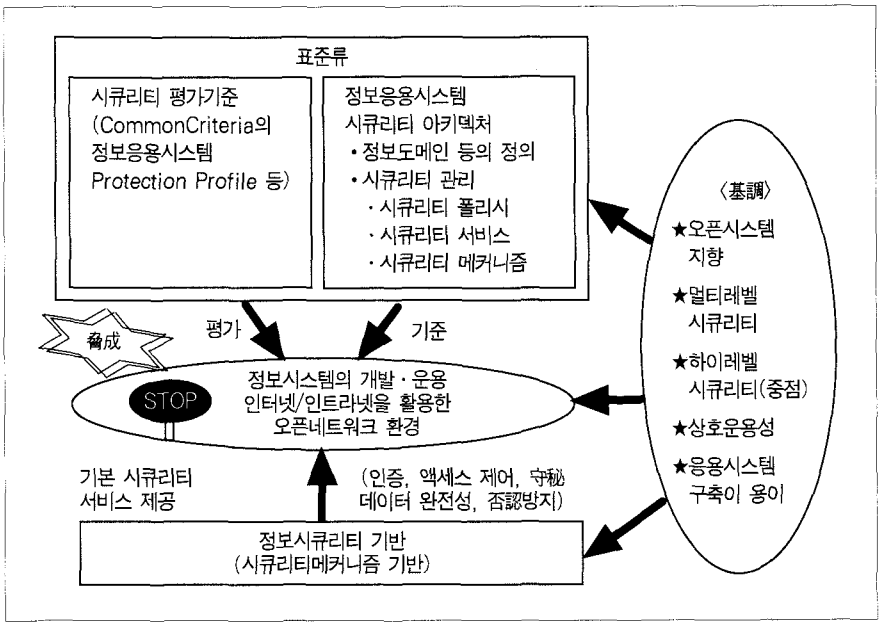
이밖에도 虹彩 · 망막 · 얼굴 등 여러 가지 인식수단이 있는데 용도 · 분야 · 환경 그리고 필요로 하는 시큐리티의 정도에 따라 조합하여 사용되는 케이스가 있다.

이것들은 인간의 감각 · 인식을 대행하는 수단이지만 이 이외에 인간의 감각 · 인식을 서포트하여 그 힘이 미치는 범위를 공간적 · 시간적으로 확대시키는 기능이 있다. 특히 안전 · 방범시큐리티에서 현저하게 요구되는 인적감시에 못지 않는 코스트효율, 그리고 인적으로는 이제까지는 불가능하였던 부분도 감시할 수 있게 된다.

감시카메라시스템에 의한 영상감시, 센서(광, 적외선, 초음파, 마이크로파)에 의한 침입검지, 시설과 모니터센터를 네트워크로 묶는 원격감시 등이 있다.

사무실, 호텔, 점포, 어미니티 에어리어, 엘리베이터, 주차장 등이 있는 대형화된 고층 빌딩용의 대규모 종합네트워크 집중감시시스템에 대한 요구가 있다. 앞으로는 디지털회선의 보급으로 다른 OA설비와 접속되어 상호 데이터를 공유하는 시스템으로의 전개, 나아가 정보시큐리티와의 통합강화가 더욱더 필요하게 된다.

고속도로 요금수집시스템의 무인화를 포함하는 광역교통정보 · 제어시스템 등의 경우도 마찬가지이다.

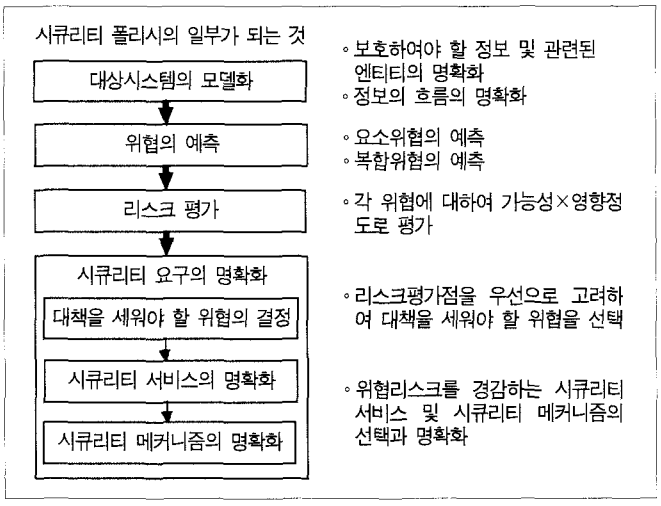


〈그림 4〉 정보시큐리티의 틀짜기

6. 應用시스템

앞으로의 응용시스템을 구축함에 있어서 정보시큐리티의 동향은 다음과 같이 집약된다. 즉 오픈시스템 지향 멀티레벨 시큐리티(다른 기밀구분 데이터가 공존한다. 복수의 정보도메인/복수의 시큐리티정책을 서포트), 하이레벨 시큐리티, 상호운용성(다른 시큐리티시스템과의 통신 및 상호인증), 시스템 구축과 메인터넌스의 용이함 등이 요구된다. 그리고 이것들을 실현하기 위해서는 그림 4에 표시하는 것과 같이 시큐리티 평가기준, 시큐리티 아키텍처, 시스템구축수단인 정보시큐리티의 기술, 그리고 제품의 기반 정비 등이 전제 조건으로서 요구된다.

또 대상이 되는 업무, 응용시스템의 리스크 분석이 시스템 설계에 앞서서 이루어져야만 한다. 그림 5에 그 어프로치를 나타내었다.



〈그림 5〉 리스크 분석방법

7. 맺음말

암호 · 시큐리티의 기술/제품은 종래에는 일부 특정한 유저마켓에 한정되어 있었으나 앞으로는 본격적으로 사회 · 공공의 인프라에 널리 침투하여 실용화 단계로 접어들 것으로 보인다. 따라서 기술, 제품의 급속한 진화, 코스트저감, 사용법과 사용자측을 포함한 시스템의 총체적인 시큐리티의 실현에 대한 요구가 보다 더 심해질 것으로 생각된다. ㅈ