# 정 보 통 신

# 용 어 해 설

### 이중 사용(二重使用) double-spending [관리운용]

전자 화폐를 불법 복제하여 무단으로 반복 사용하는 것. 전자 화폐는 그 자체가 하나의 가치를 가진 디지털 정보이다. 디지털 정보는 종이 문서와는 달리 복제가 쉽고, 또한 그 원본 및 사본의 구별이 불가능하다. 따라서 전자화폐 시스템 설계시 가장 중요하게 고려해야 될 부분으로, 이중 사용 문제에 대한 해결 방법에는 전자 화폐 내에 삽입되어 있는 사용자의 ID를 추출하여 이중 사용자를 추적하는 사후 검출 방법과 스마트 카드와 같이 같은 정보가 반복적으로 이용되는 것을 감지함과 동시에 작동을 중지시키는 사전 검출 방법이 있다.

### 접근 제어 엔트리(接近制御-) access control entry [ACE] [컴퓨터]

자원 접근 권한을 부여하는 접근 제어 목록(ACL)의 접근 진입점. 일단의 접근 권한과 하나의 보안 식별자(SID)로 구성된 것으로, 접근 권한의 허용, 거부, 검사 등 보안 사항을 식별하기 위해 32비트 접근 마스크를 사용한다.

### 접근 토큰(接近-)
### access token [컴퓨터]

로그온 수행시 필요한 보안 정보가 들어 있는 일종의 객체. 로그온 할 때 만들어지며 프로세스마다 하나의 토큰 사본이 필요한 것으로, 사용자, 사용자 그룹 및 사용자의 특권을 식별하며, 시스템에서 보안 객체의 접근 및 시스템 운용 제한을 위해 사용된다. 접근 토큰에는 윈도즈 커널에서만 만들어지는 1차(primary) 토큰과 클라이언트 프로세스의 보안 정보 캡쳐용으로 만들어지는 위장(impersonation) 토큰이 있다.

### 카드 검증 값(-檢證-)
### Card Verification Value [CVV] [관리운용]

신용 카드의 앞면 혹은 뒷면에 새겨진 검증용 숫자. 3~4개의 숫자로 보통 카드 번호 다음에 붙고, 사용하는 동안에는 절대로 변경되지 않으며, 카드 소지자를 식별하는 보안 기능을 갖는다. 신용 카드의 위·변조, 타인 명의 카드 발급 등 부정 사용 방지를 위해 사용되는 기능이다.

### 인증 코드(認證-)
### Authenticode [관리운용]

인터넷 익스플로러가 제공하는 보안 기술의 하나. 내려 받기 할 파일이나 프로그램의 원본이 안전함을 보장하기 위해 프로그램 파일을 만든 다음 파일에 디지털로 서명하는 것으로, 데이터 자체에 특수한 디지털 서명 문자열로 부호화한다. 기본적으로 서명은 서명한 사람이 그 파일을 만들었다는 것을 인증한다.

### 암호 파일 시스템
### Cryptographic File System [CFS] [컴퓨터]

파일 시스템과 암호화된 파일 접근을 통해 시스템 수준의 안전한 저장 장치를 지원하는 시스템. 유닉스 파일 시스템에서 사용되는 암호 서비스로서 디렉터리에 있는 암호 키를 사용해 파일을 암호화하고 해독하며, 평문은 디스크 저장이나 파일 서버 전송이 전혀 불가능하다. 워크스테이션에 고도의 보안성을 제공하기 위해 데이터 암호 표준(DES)과 부호록(codebook) 암호 모드를 조합시킨 방법을 채택하고 있다. 네트워크 파일 시스템(NFS)과 같은 원격 파일서버를 포함한 완전한 저장 장치를 위한 파일 시스템에서 사용된다.

### 인증 기관(認證機關)
### Certificate Authority [CA] [관리운용]

보안 적격 여부 및 메시지 암호화를 위한 공개키의 발급과 관리를 담당하는 네트워크상의 기관. 공개키 기반 구조의 일부로서 디지털 인증서 신청자에 의해 제공되는 정보를 검증하기 위한 등록 기관(RA)과 함께 보안성 등을 검사하고, 등록 기관에 의해 요구자의 정보가 입증되면 인증 기관은 인증서를 발급한다. 인증서는 대개 요구자의 공개키, 인증서의 유효 기간, 요구자의 이름 및 기타 공개키의 신청자에 관한 다른 정보들이 들어있다.

### 인증서 정책(認證書政策)
### certificate policy [관리운용]

공개키 기반 구조(PKI)에서 특정 공동체에 의하여 사용될 인증서 발급 정책. 인증서 사용 목적, 공표 방법 등 인증서와 관련된 일련의 규정을 의미하는 정책으로서 인증 업무 준칙(CPS)으로 구체화되며, 각 국은 자체 PKI에 맞는 서로 다른 인증 업무 준칙과 인증서 정책을 가지고 있다. 인증서 정책을 통해 전자 통신을 수행하는 정부와 민간의 사용자는 자신이 디지털 서명한 메시지가 인증서를 참조함으로써 검증된다.

### 인증 기관 인증서(認證機關認證書)
### Certification Authority Certificate [CA Certificate] [관리운용]

하나의 인증 기관이 다른 인증 기관에게 발행한 인증서. 인증 기관에서 발급한 전자 인증서의 확인을 위해 인증 기관 자체의 인증서가 필요하다. 인증 기관은 모든 인증서에 자체 개인 키를 사용하고, 그러기 위한 인증 기관 공개키는 인증 기관 인증서에 포함되어 있다. 브라우저는 인증 기관의 개인 키로 서명된 인증서를 확인하기 위해 인증 기관 인증서를 가져야 한다.

### 패턴 인식(표준)
### pattern recognition [기초]

컴퓨터를 사용해서 화상, 문자, 음성 등을 인식하는 것. 문자 인식, 음성 인식 및 화상 인식 등이 있다. 패턴 인식시스템은 일반적으로 특징 추출과 패턴 정합 부분으로 되어있는데, 특징 추출은 화상 등의 이미지데이터나 음성 등의 파형데이터를 분석해서 그 데이터의 고유 특징(패턴)을 추출한다. 시스템은 인식 대상 패턴을 표준 패턴으로 작성해 두었다가, 인식시에 이 표준 패턴과 입력 패턴을 비교(패턴 정합)해서 표준 패턴과 가장 유사한 것을 인식 결과치로 한다. 문자 인식은 인식 대상으로 하는 문자의 종류와 인식 방법으로 분류되며, 음성 인식은 연속적인 문장 음성 인식을 개발 대상으로 한다. 화상 인식은 이미지 데이터의 색이나 농담, 거리 등으로부터 점이나 선, 특정 영역, 배경 등을 추출해서 대상이 되는 물체 등을 인식한다.

### 인프라넷(표준)
### infranet [통신망]

인터넷 망의 기반 구조. 인터넷에서 인프라넷은 인터넷 프로토콜을 사용한 데이터패킷 교환 공중 전화망 및 사설망 기반 구조를 포함하며, 인프라넷 구축시 트렁크 망은 SONET/SDH 또는 파장 분할 다중 방식(WDM)망을 이용한다.

### 디지털 인증서(표준)
### digital certificate [관리운용]

인터넷 웹 상에서 비즈니스 또는 거래를 할 때 거래 상대방을 믿고 신뢰할 수 있도록하는 일종의 전자 보증서. 특정의 인증기관에서 발급하며, 내용은 인증서의 소유자 이름, 유효기간, 소유자의 전자 서명을 확인할 수 있는 공개 키, 그리고 이러한 내용이 사실임을 증명하는 인증기관의 전자 서명 값 등을 포함한다.

### UML(표준)
### Unified Modeling Language [데이터통신]

객체 지향분석/설계용의 모델링언어. 종래의 객체 지향 방법론과 함께 제안되어 모델링 언어 표기법의 표준화를 목적으로 한 것이다. 주로 미국의 rational software사에서 방법론의 통일과 표준화 작업에 전념한 결과 1997년 11월에 UML 1.1이 객체 관리 그룹(OMG)에 의해 표준으로 채택되었다. UML은 방법론이 아닌 S/W 개발에 사용되는 다이어그램을 정의하는 것으로, S/W 개발시 산출물들을 비주얼하게 제공함으로써 개발자와 고객 또는 개발자 상호간의 의사 소통을 원활하게 할 수 있으며, 산업계 표준으로 채택되었기 때문에 UML을 적용한 시스템은 신뢰성이 있다. →객체지향설계